PARECER Nº , DE 2007

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

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

O PLS nº 137, de 2000, de autoria do Senador Leomar Quintanilha, consiste em apenas um artigo, além da cláusula de vigência, e visa a aumentar em até o triplo as penas previstas para os crimes contra a pessoa, o patrimônio, a propriedade imaterial ou intelectual, os costumes, e a criança e o adolescente, na hipótese de tais crimes serem cometidos por meio da utilização da tecnologia de informação e telecomunicações.

O PLS 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 n° 76, de 2000 – por ser esse mais abrangente e mais antigo –, com proveito parcial dos demais, na forma do Substitutivo oferecido,

que logrou ser aprovado perante a Comissão, constituindo-se em Parecer, que integra este processado.

Em síntese, o Substitutivo pretende:

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

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

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

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

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

f) inserir parágrafo único no art. 298 do CP, para equiparar a documento particular o cartão de crédito ou débito ou qualquer dispositivo portátil de armazenamento ou processamento de informações;

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

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

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

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

Não foram apresentadas emendas.

II – ANÁLISE

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

O tema é atual e merece a devida atenção do Congresso Nacional. Segundo recentes dados divulgados pelo Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (cert.br), as tentativas de fraudes pela internet no Brasil cresceram 53% em 2006. Em 2005, foram registradas 27,3 mil tentativas de fraudes pela rede. Em 2006, foram 41,8 mil. Os números, frise-se bem, podem ser muito maiores que esses, dado que o cert.br considera apenas os dados reportados espontaneamente pelos usuários e administradores de redes.

Ao todo, o cert.br recebeu, no ano passado, 197 mil incidentes relacionados à internet, alta de 191% em relação a 2005. Os principais alvos são os usuários interessados em usar bancos ou fazer compras pela rede mundial de computadores. A estimativa é de que os bancos perdem mais de R$ 300 milhões por ano em fraudes virtuais.

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

Estes aperfeiçoamentos foram devidamente analisados pelo mesmo grupo de voluntários, aos quais registramos nossos agradecimentos, que colaboraram informalmente na construção do Substitutivo apresentado na Comissão de Educação desta casa legislativa. Lá, inicialmente, foram contatados quase cem profissionais de várias especialidades correlatas com a matéria ora em discussão, alem de oficiais superiores das três forças armadas, que cuidaram da alteração do Código Penal Militar, e ao final resumiu-se a um grupo de especialistas voluntários que, com o uso intensivo da internet, logrou concluir pelo texto do substitutivo afinal aprovado.

Analisadas as sugestões, na sua maioria de redação para clareza e concisão, concluímos que a matéria, complexa, abrangente, tratando de crimes contra a pessoa, contra o patrimônio e contra serviços públicos, requer um novo substitutivo, que pode ser comparado com aquele da Comissão de Educação, por quem tiver interesse no tema. Assim, passamos a descrever as alterações, supressões e inclusões.

Começamos por alterar a ementa da Lei para nela incluir a indicação da alteração da Lei nº 9.296, de 24 de julho de 1996 (que cuida das interceptações de comunicações telefônicas, regulamentando o inciso XII, parte final, do art. 5º da Constituição Federal), a indicação da alteração do Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal), a indicação da alteração da Lei nº 10.446, de 8 de maio de 2002 (que dispõe sobre infrações penais de repercussão interestadual ou internacional que exigem repressão uniforme), e a indicação da alteração da Lei nº 8.078, de 11 de setembro de 1990 (Código do Consumidor).

Incluímos um novo art. 1º, renumerando-se os demais, para cumprir o que determina o art. 7º, da Lei Complementar nº 95, de 26 de fevereiro de 1998, segundo o qual o primeiro artigo do texto "indicará o objeto da lei e o respectivo âmbito de aplicação".

Recebemos ponderações de que nem tudo é digital embora seja eletrônico, como, por exemplo, alguns dispositivos de comunicação, com componentes eletrônicos mas analógicos.

Assim, substituímos toda referência aos termos "eletrônico" e "eletronicamente" pelas expressões abrangentes "eletrônico ou digital ou similar" ou "eletrônica ou digitalmente ou de forma equivalente", respectivamente, em todo o corpo do Substitutivo, deixando o texto mais consoante à realidade da tecnologia, pretendendo com isso maior longevidade e adaptabilidade para o texto da norma em apreço.

No novo art. 154-A do Código Penal, e no seu correspondente novo art. 339-A do Código Penal Militar, incluímos a expressão "ou sistema informatizado" no título do artigo, dando-lhe coerência com o seu texto. Ainda, substituímos a expressão "indevido" pela expressão "não autorizado" e a expressão "indevidamente" pela expressão "sem autorização do legítimo titular, quando exigida:", colocada ao final do texto, para definir melhor o tipo. Outrossim, retiramos a expressão "indevidamente" do texto do § 1º do artigo.

Nestes artigos incluímos ainda dispositivos para ressalvar os profissionais autorizados que fazem a "defesa digital", a prevenção, a análise e a resposta aos acessos indevidos.

Para maior precisão e clareza, no novo art. 154-B do Código Penal, e no seu correspondente novo art. 339-B do Código Penal Militar, trocamos de posição na oração a expressão "dado ou informação obtida", e incluímos a ação de "obter" o dado ou a informação. Trocamos a expressão "indevidamente" pela expressão "sem autorização do legítimo titular, quando exigida", definindo melhor o tipo.

Para maior clareza, incluímos também a manutenção consigo do dado ou informação obtido com autorização por prazo definido e que tenha expirado, prática comum daquele que se infiltra, obtém as informações que virá a usar uma vez fora do ambiente atacado.

Acrescentamos a majorante de um terço da pena se o dado ou informação obtida indevidamente ou sem autorização é fornecido pela rede de computadores ou em qualquer outro meio de divulgação em massa.

Nas definições constantes do novo art. 154-C do Código Penal, e do seu correspondente novo art. 339-C do Código Penal Militar, fizemos as seguintes alterações:

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

– na definição de "Sistema Informatizado" substituímos a expressão "eletronicamente" pela expressão "eletrônica ou digitalmente ou equivalente", incluímos a expressão "capturar" e suprimimos a expressão "rede de computadores ou internet", que passou a ser objeto de definição específica;

– retiramos a definição de "Identificação de Usuário", bem como a definição de "Autenticação de Usuário", que deixam de ser necessárias no texto da norma, já que os artigos que as citavam foram convolados em normas administrativas;

– incluímos a definição de "Rede de Computadores", para nela incluir a definição de internet, a rede mundial de computadores, reclamada por alguns dos colaboradores na elaboração do Substitutivo, e definindo todas as demais redes de computadores, locais, regionais, nacionais, privadas ou públicas. Na definição, uma rede de computadores é entendida como um conjunto de computadores e dispositivos de comunicação, governados entre si, de comum acordo, por um conjunto de regras, códigos e formatos agrupados em protocolos. Assim, ela é destacada de "sistema informatizado", conceito mais abrangente, que inclui qualquer sistema, alguns deles não dispondo de meios para identificar e autenticar usuários e muito menos para armazenar os dados de conexão, conforme requeridos pelos processos de investigação penal;

– incluímos a definição de "Defesa Digital", para que se possa isentar de pena, em alguns dos novos crimes, a manipulação de código malicioso por agente técnico ou profissional habilitado, em proveito próprio ou de seu preponente, e sem risco para terceiros, de forma tecnicamente documentada e com preservação da cadeia de custódia no curso dos procedimentos correlatos, a título de teste de vulnerabilidade, de resposta a ataque, de frustração de invasão ou burla, de proteção do sistema, de interceptação defensiva, de tentativa de identificação do agressor, de exercício de forense computacional e de práticas gerais de segurança da informação;

– incluímos a definição de "código malicioso", qual seja o conjunto de instruções e tabelas de informações ou programa de computador ou qualquer outro sistema capaz de executar uma seqüência de operações que resultem em ação de dano ou em obtenção não autorizada de informações contra terceiro, de maneira dissimulada ou oculta, transparecendo tratar-se de ação de curso normal;

– incluímos as definições de "dados informáticos" e "dados de tráfego", para prover maior harmonia com a Convenção do Cibercrime, facilitando assim a participação do Brasil, se esse for o seu interesse.

No novo art. 154-D, *caput*, do Código Penal, e no seu correspondente novo art. 339-D, *caput*, do Código Penal Militar incluímos também as condutas de "utilizar" e de "comercializar" sem autorização ou para fim diferente da sua constituição, o conteúdo de um banco de dados. Para a decisão de autorizar a divulgação de informações contidas em banco de dados, incluímos a expressão "nos casos previstos em lei," dando maior clareza à norma.

Renumeramos o parágrafo único destes artigos como § 1º, e acrescentamos o § 2º com a majorante de um terço da pena se o crime ocorre em rede de computadores, dispositivo de comunicação ou sistema informatizado, ou em qualquer outro meio de divulgação em massa.

Em relação à "preservação dos dados de conexões realizadas", do novo art. 154-E do Código Penal e do seu correspondente novo art. 339-E, do Código Penal Militar, os artigos foram excluídos e as penas foram transformadas em multas administrativas, constantes do final do Substitutivo, com ênfase na finalidade da guarda dos dados, deixando claro que se tutela a justiça, afirmando-os como dados de valor probatório, aptos à identificação do usuário e da conexão quando da ocorrência de crime.

Na nova redação dos dispositivos a eles correspondentes retiramos a expressão "e comunicações", considerada demasiado abrangente, pois o que se pretende são os dados de conexões realizadas e não aqueles da continuidade da conexão, o que onera sem necessidade os operadores do sistema.

Reduzimos a lista de informações a serem guardadas, significando menor volume de arquivamento para os operadores, o que também acontece com a redução do prazo de guarda de "cinco" para "três" anos, que é a recomendação do Comitê Gestor da Internet do Brasil (CGI.br), prazo considerado suficiente para os trabalhos de investigação quando necessários.

Por sugestão recebida para melhor tipificação, incluímos artigo ao Substitutivo, renumerando-se os demais, para com ele acrescentarmos o inciso V ao § 4º do art. 155 do Código Penal e acrescentarmos o inciso V do § 6º ao seu correspondente art. 240 do Código Penal Militar. Ambos tratam do crime de "furto qualificado", que tem a pena definida como de reclusão de dois a oito anos, e multa, se o crime é cometido, por exemplo, com emprego de chave falsa. Adicionamos o inciso com as orações alternativas: "mediante uso de rede de computadores, dispositivo de comunicação ou sistema informatizado ou similar, ou contra rede de computadores, dispositivos de comunicação ou sistemas informatizados e similares".

No novo art. 163-A do Código Penal, e no seu correspondente novo art. 262-A do Código Penal Militar, aperfeiçoamos a redação, substituindo no título a expressão "vírus" por "código malicioso", considerada mais adequada, pois passa a abranger qualquer código malicioso criado, inserido ou difundido, que se reproduz automaticamente ou não, ou que toma controle do equipamento sem autorização do seu usuário, causando-lhe dano na destruição, ou no impedimento de uso ou no mau funcionamento do equipamento. Assim, incluímos a conduta de fazer a rede de computadores, o dispositivo de comunicação ou o sistema informatizado funcionar para o agente criminoso sem a autorização do usuário – situação essa que, no jargão técnico, é a de transformar o equipamento em um "zumbi".

A definição do novo tipo começa pela forma mais simples de dano ao criar, inserir e difundir código malicioso, para nos dois parágrafos seguintes ser qualificado pela intenção de causar dano, e novamente qualificado pela apuração do resultado do dano, com o correspondente progressivo agravamento da pena.

Nestes artigos renumeramos o parágrafo único como § 1º e incluímos ainda dispositivos para ressalvar os profissionais autorizados que fazem a "defesa digital", a prevenção, a análise e a resposta aos acessos indevidos.

Alteramos a localização do novo tipo de "difusão de código malicioso" por fraude, anteriormente o novo art. 266-A do Código Penal, ficando melhor codificado no novo art. 171-A (do Título II – Dos Crimes contra o Patrimônio – Capítulo VI – Estelionato e outras Fraudes). A motivação para a mudança foi que o Capítulo anterior (do Título VIII – Dos Crimes contra a Incolumidade Pública – Capítulo II – Dos Crimes contra a Segurança dos Meios de Comunicação e Transporte e outros Serviços Públicos) trata de crimes contra "serviços públicos" e desta forma o novo tipo alcançaria apenas rede de computadores, dispositivo de comunicação e sistema informatizado de acesso público, como computadores de acesso público, terminais de bancos etc, deixando de alcançar todos os demais citados de acesso privado. Ademais o tipo de fraude se realiza com o objetivo direto ou indireto de obter ganho econômico, daí a tipificação como estelionato.

Alteramos a pena do novo tipo de "difusão de código malicioso", do novo art. 171-A do Código Penal e no seu correspondente novo art. 339-A do Código Penal Militar, passando de detenção de um a dois anos para reclusão de um a três anos, pois a pretensão dos autores da difusão de código malicioso é a fraude, que pode levar ao "furto qualificado por acesso indevido" (arts. 4º e 11 do PLS), igualando-a à pena que se aplica ao crime tipificado no novo art. 163-A. Nestes artigos, renumeramos o parágrafo único como § 1º e acrescentamos o § 2º, para ressalvar a ação dos profissionais que fazem a "defesa digital", a prevenção, análise e resposta aos ataques tipificados.

Acrescentamos à alteração do art. 266 do Código Penal as expressões "informático, dispositivo de comunicação, rede de computadores, sistema informatizado", seja para adequação aos termos já dispostos na Lei 9.296, de 1996, e aos termos do art. 154-C do Substitutivo, seja para nele incluir como tipo penal "o ataque a rede de computadores ou sistema informatizado", como, por exemplo, o *DoS* (*Denial-of-Service attack*), o *DDoS* (*Distributed-Denial-of-Service attack)* e outros equivalentes.

Alteramos o parágrafo único do art. 298 do Código Penal, o qual se pretende acrescentar, para substituir a expressão "armazenamento ou processamento" pela expressão "captura, armazenamento, processamento ou transmissão" que é uma tipificação clara nos dispositivos de comunicação ou sistemas informatizados, para maior abrangência do texto.

Alteramos a localização do novo tipo de "difusão de código malicioso" por fraude, anteriormente o novo art. 266-A do Código Penal, ficando melhor codificado no novo art. 171-A (do Título II – Dos Crimes contra o Patrimônio – Capítulo VI – Estelionato e outras Fraudes). A motivação para a mudança foi que o Capítulo anterior (do Título VIII – Dos Crimes contra a Incolumidade Pública – Capítulo II – Dos Crimes contra a Segurança dos Meios de Comunicação e Transporte e outros Serviços Públicos) trata de crimes contra "serviços públicos" e desta forma o novo tipo alcançaria apenas rede de computadores, dispositivo de comunicação e sistema informatizado de acesso público, como computadores de acesso público, terminais de bancos etc, deixando de alcançar todos os demais citados de acesso privado. Ademais o tipo de fraude se realiza com o objetivo direto ou indireto de obter ganho econômico, daí a tipificação como estelionato.

Alteramos a pena do novo tipo de "difusão de código malicioso", do novo art. 171-A do Código Penal e no seu correspondente novo art. 339-A do Código Penal Militar, passando de detenção de um a dois anos para reclusão de um a três anos, pois a pretensão dos autores da difusão de código malicioso é a fraude, que pode levar ao "furto qualificado por acesso indevido" (arts. 4º e 11 do PLS), igualando-a à pena que se aplica ao crime tipificado no novo art. 163-A. Nestes artigos, renumeramos o parágrafo único como § 1º e acrescentamos o § 2º, para ressalvar a ação dos profissionais que fazem a "defesa digital", a prevenção, análise e resposta aos ataques tipificados.

Acrescentamos à alteração do art. 266 do Código Penal as expressões "informático, dispositivo de comunicação, rede de computadores, sistema informatizado", seja para adequação aos termos já dispostos na Lei 9.296, de 1996, e aos termos do art. 154-C do Substitutivo, seja para nele incluir como tipo penal "o ataque a rede de computadores ou sistema informatizado", como, por exemplo, o *DoS* (*Denial-of-Service attack*), o *DDoS* (*Distributed-Denial-of-Service attack)* e outros equivalentes.

Alteramos o parágrafo único do art. 298 do Código Penal, o qual se pretende acrescentar, para substituir a expressão "armazenamento ou processamento" pela expressão "captura, armazenamento, processamento ou transmissão" que é uma tipificação clara nos dispositivos de comunicação ou sistemas informatizados, para maior abrangência do texto.

Com o art. 21 do Substitutivo, passamos a tratar das obrigações do responsável pelo provimento de acesso a uma rede de computadores. Mantivemos a obrigação da preservação, por eles, das informações relativas às conexões realizadas, pelo prazo de três anos, em redação mais simples e concisa.

Em nível latino-americano registre-se que Lei Argentina de 2003 fixa o prazo de dez anos para a guarda destas informações. E ainda que recentemente chegou ao Congresso Americano projeto de lei propondo a retenção por prazo indeterminado destas informações.

Recentemente a imprensa da Coréia do Sul registrou que foi aprovada pela Assembléia Nacional daquele país, no último dia 22 de dezembro, a revisão do chamado "Ato de Incentivo à Utilização das Redes de Informação e Comunicação e de Proteção à Informação", determinando que os usuários da Internet preencham cadastro ao visitarem sites com mais de 100 mil acessos diários, no chamado "Sistema de Nome Real" (Internet Real-Name System, em livre tradução).

A ofensiva do governo em rediscutir o tema foi respaldada por uma série de pesquisas realizadas junto a internautas, nos principais websites do país. De acordo com o Korea Times, dos 7.909 pesquisados junto aos usuários do Naver, maior portal de Internet coreano, 65% apoiariam o registro de seus dados verdadeiros na Web. Já 80% dos visitantes do Yahoo, num universo de 1.631 entrevistados, seriam a favor do Sistema de Nome Real. Por sua vez, o Instituto Gallup detectou uma aceitação de 75,6% dos pesquisados on-line.

A nova legislação coreana prevê a obrigatoriedade do registro, com dados verdadeiros, inclusive documentação de identidade, dos usuários de Internet em sites com mais de 100 mil acessos diários, quando encaminharem mensagens on-line ou comentários de informações divulgadas em portais, páginas de notícias e de imprensa, bem como de entidades governamentais.

O principal pressuposto dessa regra seria permitir que os provedores de conteúdo identificassem, quando necessário, os remetentes de determinados comentários. Dessa forma, os administradores dos sites poderiam bloquear, por até 30 dias, mensagens consideradas potencialmente controversas ou difamatórias. Esses provedores estariam sujeitos a multas de até 30 milhões de wons (cerca de 30 mil dólares), caso não disponibilizassem o sistema de registro.

Cumpre lembrar aqui a confusão (ou desinformação) que se estabelece acerca da relação entre liberdade de expressão e anonimato, ambos possíveis na internet (o anonimato representado pela não-identificação e a não-autenticação do usuário).

Ora, se o fato de emitir para alguém uma carteira de habilitação para dirigir veículos automotores não limita o seu direito constitucional de ir e vir, da mesma forma a identificação do usuário de uma rede de computadores não o impede de manifestar-se pela rede.

Importante frisar que a própria Constituição Federal determina, no art. 5º, inciso IV, que "é livre a manifestação do pensamento, sendo vedado o anonimato".

O art. 21 do Substitutivo apenas reafirma esta norma constitucional, e consagra prática mundial de usos e costumes de todos quantos tem na rede de computadores o seu instrumento de prestação de serviços, diferenciando pela quantidade ou pelo tipo de informação requerida quando do acesso, pois quem presta serviço quer saber de quem cobrará economicamente pelos serviços prestados.

Esse aspecto fez parte de comentário recente do pesquisador Vint Cerf, criador dos principais protocolos da internet, na resposta à primeira pergunta em entrevista à imprensa nacional:

> *Nos Estados Unidos é comum que o internauta forneça algum número de identificação para ter acesso em lugares públicos como hotspots, como número de cartão de crédito ou endereço. Em muitos casos, além do cartão você deve fornecer seu endereço para provar que é realmente a pessoa que diz ser. De certa forma, os provedores de acesso à internet já possuem informações confidenciais dos internautas. Se você assina um serviço de banda larga é muito pouco provável que o provedor forneça este serviço sem saber quem você é, ou ter pelo menos o número do seu cartão de crédito, seu endereço e sua conta bancária. Diria que, em muitas instâncias do acesso à internet, os provedores já possuem um montante de informações pessoais sobre os usuários.*

Na segunda resposta da mesma matéria, ele comenta os dados que os provedores deveriam fornecer por requisição judicial, e termina mencionando que os usuários pensam que são anônimos, mas não o são, pois os provedores tem vários dados sobre cada um:

> *O interessante desta questão é avaliar em quais condições os provedores deveriam fornecer informações para o suporte à lei. Não estou familiarizado com a lei brasileira, mas nos Estados Unidos você tem ordens judiciais para obter certos tipos de informação. De certa forma, podemos entender que não deixa de ser um pedido razoável. Existe o mesmo processo com o telefone. Provavelmente, em muitos casos judiciais, ligações e mensagens telefônicas são solicitadas como provas em tribunais. Minha primeira impressão é que isso não parece terrivelmente diferente das práticas aplicadas por aí. Temos de imaginar que se isso for aprovado de alguma forma pode parecer mais ameaçador para os internautas que acreditavam ser mais anônimos do que são. E eles não são. Acho certo dizer que, para a maioria dos provedores que cobram pelos serviços, existem de fato várias formas de rastrear e descobrir quem você é. Até em universidades você precisa fazer um registro antes de acessar a rede.*

É do que trata, por exemplo, recente decisão do Superior Tribunal de Justiça (STJ). O Tribunal da Comarca de Düsseldorf, República Federal da Alemanha, solicitou ao Brasil, mediante carta rogatória, que a empresa Universo *On Line* informasse os dados de pessoa que, em fevereiro de 2004, bloqueou o acesso aos sites atendidos pela empresa "Online-forum". O intimado apresentou impugnação invocando o princípio constitucional da inviolabilidade de dados, previsto no art. 5º, XII, da CF, que, segundo alegou, impediria a quebra do sigilo de dados cadastrais. O ministro Barros Monteiro proferiu importante decisão nos seguintes termos (Carta Rogatória nº 297 –2005/0010755-8, em 18/09/2006):

> ***Esta Corte já proferiu decisão no sentido de que o fornecimento de dados cadastrais, como o endereço p. ex., não está protegido pelo sigilo**, conforme se verifica na ementa a seguir reproduzida:*
>
> *"Imposto de renda. Informações. Requisição. Os elementos constantes das declarações de bens revestem-se de caráter sigiloso que não deve ser afastado se não em situações especiais em que se patenteie relevante interesse da administração da Justiça. Tal não se configura quando se trate apenas de localizar bens para serem penhorados, o que é rotineiro na prática forense. Injustificável, entretanto, negar-se o pedido na parte em que pretende obter dados pertinentes ao endereço do executado. Em relação a isso não há motivo para sigilo" (RESP 83824/BA, relator Ministro Eduardo Ribeiro, DJ 17.5.99) (grifou-se).*

A respeito do assunto, cabe mencionar o estudo de Tércio Sampaio Ferraz Júnior em seu trabalho "Sigilo de Dados: O Direito à Privacidade e os Limites à Função Fiscalizadora do Estado' (Revista da Faculdade de Direito USP, vol. 88, 1993, p. 449), ao explanar sobre o alcance da proteção à vida privada:

"Pelo sentido inexoravelmente comunicacional da convivência, a vida privada compõe, porém, um conjunto de situações que, usualmente, são informadas sem constrangimento. São dados que, embora privativos — como o nome, endereço, profissão, idade, estado civil, filiação, número de registro público oficial etc, condicionam o próprio intercâmbio humano em sociedade, pois constituem elementos de identificação que tornam a comunicação possível, corrente e segura. Por isso, a proteção desses dados em si, pelo sigilo, não faz sentido. *Assim, a inviolabilidade de dados referentes à vida privada só tem pertinência para aqueles associados aos elementos identificadores usados nas relações de convivência, as quais só dizem respeito aos que convivem. Dito de outro modo, os elementos de identificação só são protegidos quando compõem relações de convivência privativas: a proteção é para elas, não para eles. Em conseqüência, simples cadastros de elementos identificadores (nome, endereço, R.G., filiação, etc.) não são protegidos. Mas cadastros que envolvam relações de convivência privada (por exemplo, nas relações de clientela, desde quando é cliente, se a relação foi interrompida, as razões pelas quais isto ocorreu, quais os interesses peculiares do cliente, sua capacidade de satisfazer aqueles interesses, etc) estão sob proteção. Afinal, o risco à integridade moral do sujeito, objeto do direito à privacidade, não está no nome, mas na exploração do nome, não está nos elementos de identificação que condicionam as relações privadas, mas na apropriação dessas relações por terceiros a quem elas não dizem respeito".*

Não é demais evocar a jurisprudência emanada da Corte Suprema brasileira, em especial o trecho do voto proferido pelo Ministro Sepúlveda Pertence*, que também dá amparo ao acolhimento da ordem pleiteada na peça exordial:*

"Não entendo que se cuide de garantia com status constitucional. Não se trata da 'intimidade ' protegida no inciso X do art. 5º da Constituição Federal. ***Da minha leitura, no inciso XII da Lei Fundamental, o que se protege, e de modo absoluto, até em relação ao Poder Judiciário, é a comunicação 'de dados' e não os 'dados', o que tornaria impossível qualquer investigação administrativa, fosse qual fosse."****(voto proferido no MS n. 21.729-4/DF, DJ 19.10.2001)* [grifos nossos].

Esperamos, assim, que o artigo 21 do Substitutivo estimule a celebração de convênios, entre aqueles que tornam possível o acesso à rede de computadores e as organizações detentoras de informações para permitir a verificação dos dados imutáveis como nome, número de documento legalmente emitido, conforme a boa prática existente entre organizações de proteção ao crédito, as instituições financeiras, órgãos públicos e outras.

Sobre esses dados a serem compartilhados, a Constituição Federal determina no seu art. 5º, inciso XXXIII, que:

> **Art. 5º** .....
> .....
> XXXIII – todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado.

O inciso foi regulamentado pela Lei nº 11.111, de 5 de maio de 2005, não proibindo o compartilhamento de dados imutáveis como os já citados, naturalmente desde que autorizados pelo seu titular ou por lei específica, pois dispõe que:

> "**Art. 2º** O acesso aos documentos públicos de interesse particular ou de interesse coletivo ou geral será ressalvado exclusivamente nas hipóteses em que o sigilo seja ou permaneça imprescindível à segurança da sociedade e do Estado, nos termos do disposto na parte final do inciso XXXIII do *caput* do art. 5º da Constituição Federal."

Ainda a propósito, cabe lembrar aqui as recomendações constantes da Cartilha de Segurança para Internet, na sua seção 6 (Responsabilidades dos Provedores), documento editado em notável esforço de colaboração entre o Ministério Público Federal de São Paulo (MPF/SP) e o Comitê Gestor da Internet no Brasil (CGI.br), patrocinada pela Associação Brasileira dos Provedores de Internet (ABRANET), aos quais registramos aqui o nosso elogio ao resultado alcançado.

A brochura contém instruções de como proceder em caso de investigação de delito ocorrido, os modelos de documentos a serem usados para comunicar o fato delituoso às autoridades competentes, o texto completo da Convenção sobre o Cibercrime, celebrado em Budapest, a 23 de novembro de 2001, pelo Conselho da Europa. Essa Convenção foi recentemente ratificada pelo Senado dos EUA.

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

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

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

O que é importante sublinhar é a harmonia brasileira com os termos da Convenção, a correspondência entre o que ela recomenda e aquilo que está sendo proposto nos projetos de lei ao qual oferecemos o presente Substitutivo. Assim, segundo a Convenção, *a criação de legislação penal em cada Estado signatário deve tratar*:

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

– *da interceptação ou interrupção de comunicações*, objeto do art. 16 do Substitutivo;

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

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

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

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

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

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

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

– *da responsabilidade de uma pessoa natural ou de uma organização*, objeto do art. 21 do Substitutivo;

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

Resumindo, a legislação brasileira em vigor já tipifica alguns dos crimes identificados pela Convenção, como os crimes contra os direitos do autor e crimes de pedofilia, e, caso a caso, cuida de alguns outros já tipificados no Código Penal. O presente Projeto de Lei, que atualiza o nosso Código Penal, o Código do Processo Penal, o Código Penal Militar, a Lei das Interceptações Telefônicas, a Lei da Repressão Uniforme e o Código do Consumidor, coloca o Brasil em posição de destaque para que possa tratar e acordar de maneira diferenciada com os países signatários da Convenção de Budapest e outras, inclusive os EUA, país sede das maiores empresas de tecnologia da informação e sede dos maiores provedores de acesso à rede mundial de computadores.

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

Em outro documento, a "Directiva 2006/24/CE do Parlamento Europeu e do Conselho, de 15 de março de 2006, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações electrônicas publicamente disponíveis ou de redes públicas de comunicações, e que altera a Directiva 2002/58/CE", entre outras considerações preambulares, trata naquela de número 18 que "*A decisão-Quadro 2005/222/AI do Conselho, de 24 de fevereiro de 2005, relativa a ataques contra os sistemas de informação, dispõe que o acesso ilegal aos sistemas de informação, incluindo os dados neles conservados seja punível como infracção penal.*" Na consideração de número 20 cita a Convenção sobre o Cibercrime de Budapest de 2001 e a Convenção de 1981, esta sobre os dados pessoais.

Avançando, a "Directiva" define no art. 2º como dados: os "*dados de tráfego e os dados de localização bem como os dados conexos necessários para identificar o assinante e o utilizador*". No art. 5º detalha as "*Categorias de dados a conservar*", onde encontramos, no item 2 da letra *a*, que diz respeito à internet, a especificação da guarda do identificador de acesso, do nome e do endereço do assinante ou usuário, aos quais o endereço do protocolo IP, o identificador de acesso ou o número do telefone, estavam atribuídos no momento da comunicação.

Faz-se mister demonstrar a harmonia do Substitutivo com a "Directiva", que nos arts. 6º, 7º, 8º e 9º define, respectivamente, os "*Períodos de Conservação*", a "*Proteção de dados e segurança dos dados*", os "*Requisitos para o armazenamento dos dados conservados*", a "*Autoridade de controle*", previstos no art. 21 do Substitutivo, incisos I e II, e § 1º.

Desses artigos vem a recomendação de que os dados sejam conservados por um período mínimo de seis meses e não superior a dois anos. Ao final da "Directiva", vários signatários declaram que estudarão a aplicação de prazos diferenciados ou de dezoito ou de trinta e seis meses, a partir de 2007 ou 2009. No Brasil, o Comitê Gestor da Internet no Brasil (CGI.br) definiu esse prazo em trinta e seis meses. A "Directiva" recomenda ainda que a guarda deva ser criteriosa e que seja designada uma autoridade competente para a realização da auditoria a que estes dados forem submetidos regularmente.

O presente Substitutivo, ao definir as obrigações dos provedores de acesso, mostra que o Brasil o faz por sua vontade soberana, mas em consonância com a "Directiva" citada dos países do Conselho da Europa, atualizando sua legislação.

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

A propósito, em dezembro de 2006 a Comissão de Relações Exteriores e Defesa Nacional do Senado Federal (CRE) aprovou Requerimento de Informações, de minha autoria, solicitando ao Ministério das Relações Exteriores qual o posicionamento oficial do Brasil em relação à Convenção, uma vez que ele ainda não é dela signatário.

Em data recente, fomos recebidos em audiência pelo Senhor Ministro das Relações Exteriores, tratando, entre outros assuntos, da Convenção sobre o Cibercrime e a posição do Brasil.

E, ao finalizarmos este Parecer, recebemos em audiência o Senhor Chefe de Cooperação Técnica, do Departamento de Problemas Criminais, da Secretaria Geral do Conselho da Europa, que nos informou que sugeriu, à Coordenadora Geral contra o Crime Transnacional do Ministério das Relações Exteriores, o envio de carta à Secretaria Geral daquele Conselho, solicitando o acesso à Convenção pelo Brasil, para, na seqüência, o Conselho da Europa ouvir os seus Países-Membros e, havendo aquiescência destes, o Brasil poderá ser convidado a participar como País Membro.

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

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

Consoante as sugestões recebidas e respaldados pelas recomendações da Convenção sobre o Cibercrime de Budapest e da Directiva 2006/24/CE do Parlamento Europeu e do Conselho, que acabamos de descrever resumidamente, incluímos o artigo 21 ao Substitutivo que determina que o responsável pelo provimento de acesso a uma rede de computadores é obrigado a:

– manter em ambiente controlado e de segurança os dados aptos à identificação do usuário e aptos à identificação das conexões realizadas por seus equipamentos: endereços eletrônicos de origem das conexões, data, horário de início e término e referência GMT, da conexão, pelo prazo de três anos, para prover os elementos probatórios essenciais de identificação da autoria das conexões na rede de computadores, em caso de ocorrência de crime;

– tornar disponíveis à autoridade competente e por autorização expressa da autoridade judicial os dados de conexão no curso de auditoria técnica a que forem submetidos;

– fornecer os dados e informações de conexões realizadas e os dados e informações de identificação do usuário quando solicitado pela autoridade competente no curso de investigação e por autorização expressa da autoridade judicial;

– preservar imediatamente, após a solicitação expressa da autoridade judicial, no curso de investigação, os dados de conexões realizadas, os dados de identificação de usuário e o conteúdo das comunicações realizadas daquela investigação, respondendo pela sua absoluta confidencialidade e inviolabilidade;

– informar, de maneira sigilosa, à autoridade competente à qual está jurisdicionado, denúncia da qual tenha tomado conhecimento e que contenha indícios de conduta delituosa na rede de computadores sob sua responsabilidade, pois não é demais lembrar que o art. 21 do Código Penal diz que ninguém pode se escusar com o desconhecimento da lei nem do ilícito;

– informar ao usuário que aquela conexão de acesso à rede de computadores sob sua responsabilidade obedece às leis brasileiras, e que toda comunicação ali realizada será de exclusiva responsabilidade do usuário, perante as leis brasileiras;

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

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

O § 1º do art. 21 do Substitutivo remete para regulamento do Poder Executivo o detalhamento relativo aos dados de conexão, às condições de segurança de seu armazenamento, a auditoria a que serão submetidos, a autoridade competente para realizá-la, o texto a ser apresentado aos usuários e estipula um prazo de noventa dias para a sua publicação.

O § 2º determina o prazo de transição de cento e oitenta dias a partir da promulgação da lei para que os dados e procedimentos requeridos estejam disponíveis.

Os §§ 3º e 4º§ definem, respectivamente, a multa variável de dois a cem mil reais, dobrando no caso de reincidência, independentemente de indenização por danos à vítima, pelo descumprimento das obrigações e a destinação dos recursos financeiros resultantes ao Fundo Nacional de Segurança Pública (de que trata a Lei nº 10.201, de 14 de fevereiro de 2001). A multa será imposta mediante procedimento administrativo, pela autoridade judicial desatendida, considerando-se a natureza, a gravidade e o prejuízo resultante da infração.

Parte dessas disposições atende algumas das recomendações do item "6 – Responsabilidades dos Provedores", da publicação "Cartilha de Segurança para Internet", já citada, quando recomenda a publicação de alertas e informações de segurança na internet aos usuários, principalmente às crianças e adolescentes.

Por fim, o art. 22 traz dispositivo semelhante ao que temos na Lei Complementar nº 105, de 2001, que trata do sigilo bancário: não constitui violação do dever de sigilo a comunicação, às autoridades competentes, de prática de ilícitos penais, abrangendo o fornecimento de informações de acesso, hospedagem e dados de identificação de usuário, quando constatada qualquer prática criminosa. Dispositivo em plena harmonia com a jurisprudência do Supremo Tribunal Federal (STF), notadamente o voto do ministro Sepúlveda Pertence, já citado neste Parecer quando da referência à decisão do STJ na Carta Rogatória proveniente da Corte alemã.

III – VOTO

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

SUBSTITUTIVO

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

Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), o Decreto-Lei nº 1.001, de 21 de outubro de 1969 (Código Penal Militar), a Lei nº 9.296, de 24 de julho de 1996, o Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código do Processo Penal), a Lei nº 10.446, de 8 de maio de 2002, e a Lei nº 8.078, de 11 de setembro de 1990 (Código do Consumidor), para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, de rede de computadores, ou que sejam praticadas contra dispositivos de comunicação ou sistemas informatizados e similares, e dá outras providências.

O CONGRESSO NACIONAL decreta:

Art.1º Esta Lei altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), o Decreto-Lei nº 1.001, de 21 de outubro de 1969 (Código Penal Militar), a Lei nº 9.296, de 24 de julho de 1996, Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código do Processo Penal), a Lei nº 10.446, de 8 de maio de 2002, e a Lei nº 8.078, de 11 de setembro de 1990 (Código do Consumidor), para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, de rede de computadores, ou que sejam praticadas contra dispositivos de comunicação ou sistemas informatizados e similares, e dá outras providências.

Art. 2º O Capítulo V do Título I da Parte Especial do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal) fica acrescido do seguinte art. 141-A:

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

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

"Capítulo VI-A

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

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

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

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

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

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

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

§ 4º Não há crime quando o agente acessa a título de defesa digital, excetuado o desvio de finalidade ou o excesso.

Obtenąão, manutenąão, transporte ou fornecimento não autorizado de informaąão eletrônica ou digital ou similar

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

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

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

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

§ 3° Somente se procede mediante representação, salvo se o crime é cometido contra a União, Estado, Município, empresa concessionária de serviços públicos, agências, fundações, autarquias, empresas públicas ou sociedade de economia mista e suas subsidiárias.

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

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

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

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

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

IV – defesa digital: manipulação de código malicioso por agente técnico ou profissional habilitado, em proveito próprio ou de seu preponente, e sem risco para terceiros, de forma tecnicamente documentada e com preservação da cadeia de custódia no curso dos procedimentos correlatos, a título de teste de vulnerabilidade, de resposta a ataque, de frustração de invasão ou burla, de proteção do sistema, de interceptação defensiva, de tentativa de identificação do agressor, de exercício de forense computacional e de práticas gerais de segurança da informação;

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

VI – dados informáticos: qualquer representação de fatos, de informações ou de conceitos sob uma forma suscetível de processamento numa rede de computadores ou dispositivo de comunicação ou sistema informatizado, incluindo um programa, apto a fazer um sistema informatizado executar uma função;

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

Divulgação ou utilização indevida de informações contidas em banco de dados

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

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

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

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

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

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

.....

§ 4º .....

.....

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

..... (NR) "

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

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

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

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

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

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

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

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

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

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

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

§ 4º Não há crime quando a ação do agente é a título de defesa digital, excetuado o desvio de finalidade ou o excesso."

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

"**Difusão de código malicioso**

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

Pena – reclusão, de um a três anos.

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

§ 2º Não há crime quando a difusão ocorrer a título de defesa digital, excetuado o desvio de finalidade ou o excesso."

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

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

Art. 8º Os arts. 265 e 266 do Código Penal passam a vigorar com as seguintes redações:

"**Atentado contra a segurança de serviço de utilidade pública**

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

..... (NR)"

"**Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático, dispositivo de comunicação, rede de computadores ou sistema informatizado**

Art. 266. Interromper ou perturbar serviço telegráfico, radiotelegráfico, telefônico, telemático, informático, de dispositivo de comunicação, de rede de computadores, de sistema informatizado ou de telecomunicação, assim como impedir ou dificultar-lhe o restabelecimento:

..... (NR)"

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

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

.....

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

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

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

"Falsificaação de telefone celular ou meio de acesso a rede de computadores, dispositivo de comunicaação ou sistema informatizado

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

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

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

"Art. 240. .....

.....

Furto qualificado

§ 6º .....

.....

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

.....(NR) "

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

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

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

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

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

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

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

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

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

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

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

§ 4º Não há crime quando a ação do agente é a título de defesa digital, excetuado o desvio de finalidade ou o excesso."

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

"**Capítulo VII-A**

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

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

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

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

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

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

§ 3º Não há crime quando o agente acessa a título de defesa digital, excetuado o desvio de finalidade ou o excesso.

Obtenaão, manutenaão, transporte ou fornecimento não autorizado de informaação eletrônica ou digital ou similar

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

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

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

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

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

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

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

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

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

IV – defesa digital: manipulação de código malicioso por agente técnico ou profissional habilitado, em proveito próprio ou de seu preponente, e sem risco para terceiros, de forma tecnicamente documentada e com preservação da cadeia de custódia no curso dos procedimentos correlatos, a título de teste de vulnerabilidade, de resposta a ataque, de frustração de invasão ou burla, de proteção do sistema, de interceptação defensiva, de tentativa de identificação do agressor, de exercício de forense computacional e de práticas gerais de segurança da informação;

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

VI – dados informáticos: qualquer representação de fatos, de informações ou de conceitos sob uma forma suscetível de processamento numa rede de computadores ou dispositivo de comunicação ou sistema informatizado, incluindo um programa, apto a fazer um sistema informatizado executar uma função;

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

Divulgaação ou utilizaação indevida de informaações contidas em banco de dados

Art. 339-D Divulgar, utilizar, comercializar ou disponibilizar informações contidas em banco de dados com finalidade distinta da que motivou o registro das mesmas, incluindo-se informações privadas referentes, direta ou indiretamente, a dados econômicos de pessoas naturais ou jurídicas, ou a dados de pessoas naturais referentes a raça, opinião politica, religiosa, crença, ideologia, saúde física ou mental, orientação sexual, registros policiais, assuntos familiares ou profissionais, além de outras de caráter sigiloso, salvo nos casos previstos em lei ou mediante expressa anuência da pessoa a que se referem, ou de seu representante legal.

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

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

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

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

"Capítulo VIII-A

DISPOSIÇÕES GERAIS

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

Art. 15. O Capítulo I do Título VI da Parte Especial do Livro I do Decreto-Lei nº 1.001, de 21 de outubro de 1969 (Código Penal Militar), fica acrescido do art. 281-A, assim redigido:

"**Difusão de código malicioso**

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

Pena – reclusão, de um a três anos.

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

§ 2º Não há crime quando a difusão ocorre a título de defesa digital, excetuado o desvio de finalidade ou o excesso."

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

"**Art. 2º** .....

.....

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

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

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

.....

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

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

Art. 19. O art. 1º da Lei nº 10.446, de 8 de maio de 2002 passa a vigorar com a seguinte redação:

"**Art. 1º** .....

.....

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

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

"Art. 9º .....

.....

Parágrafo único. O disposto neste artigo se aplica à segurança digital do consumidor, mediante a informação da necessidade do uso de senhas ou similar para a proteção do uso do produto ou serviço e para a proteção dos dados trafegados, quando se tratar de dispositivo de comunicação, sistema informatizado ou provimento de acesso a rede de computadores ou provimento de serviço por meio dela.(NR)"

Art. 21. O responsável pelo provimento de acesso a rede de computadores é obrigado a:

I – manter em ambiente controlado e de segurança os dados de conexões realizadas por seus equipamentos, aptos à identificação do usuário e dos endereços eletrônicos de origem, da data, do horário de início e término e referência GMT, das conexões, pelo prazo de três anos, para prover os elementos probatórios essenciais de identificação da autoria das conexões na rede de computadores;

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

III – fornecer, por expressa autorização judicial, no curso de investigação, os dados de conexões realizadas e os dados de identificação de usuário;

IV – preservar imediatamente, após a solicitação expressa da autoridade judicial, no curso de investigação, os dados de conexões realizadas, os dados de identificação de usuário e as comunicações realizadas daquela investigação, respondendo civil e penalmente pela sua absoluta confidencialidade e inviolabilidade;

V – informar, de maneira sigilosa, à autoridade policial competente, denúncia da qual tenha tomado conhecimento e que contenha indícios de conduta delituosa na rede de computadores sob sua responsabilidade;

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

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

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

§ 1º Os dados de conexões realizadas em rede de computadores, aptos à identificação do usuário, as condições de segurança de sua guarda, a auditoria à qual serão submetidos, a autoridade competente responsável pela auditoria e o texto a ser informado aos usuários de rede de computadores serão definidos nos termos de regulamento.

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

§ 3º O responsável citado no *caput* deste artigo que não cumprir o disposto no § 2º, independentemente do ressarcimento por perdas e danos ao lesado, estará sujeito ao pagamento de multa variável de R$ 2.000,00 (dois mil reais) a R$ 100.000,00 (cem mil reais) a cada verificação ou solicitação, aplicada em dobro em caso de reincidência, que será imposta mediante procedimento administrativo, pela autoridade judicial desatendida, considerando-se a natureza, a gravidade e o prejuízo resultante da infração.

§ 4º Os recursos financeiros resultantes do recolhimento das multas estabelecidas neste artigo serão destinados ao Fundo Nacional de Segurança Pública, de que trata a Lei nº 10.201, de 14 de fevereiro de 2001.

Art. 22. Não constitui violação do dever de sigilo a comunicação, às autoridades competentes, de prática de ilícitos penais, abrangendo o fornecimento de informações de acesso, hospedagem e dados de identificação de usuário, quando constatada qualquer conduta criminosa.

Art. 23. Esta Lei entrará em vigor sessenta dias após a data de sua publicação.

Sala da Comissão,

, Presidente

, Relator

Oitava versão do Parecer / Substitutivo
Facsimile de cópia obtida da Comissão de Constituição e Justiça do Senado via gabinete senatorial
Brasília, DF, 27.04.2007