PARECER Nº , DE 2006

Da COMISSÃO DE EDUCAÇÃO, 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

Chegam a esta Comissão, para parecer, o Projeto de Lei da Câmara (PLC) n° 89, de 2003 (n° 84, de 1999, na origem), e os Projetos de Lei do Senado (PLS) n° 137, de 2000, e n° 76, de 2000, todos referentes a crimes na área de informática. Tramitam em conjunto, em atendimento ao Requerimento n° 847, de 2005, do Senador Renan Calheiros. Em decorrência do Requerimento n° 848, de 2005, foi extinta a urgência na tramitação do PLC n° 89, de 2005, que havia sido declarada em decorrência da aprovação do Requerimento n° 599, de 2005, de autoria da Senadora Ideli Salvatti. Os projetos de lei do Senado perdem o caráter terminativo nas comissões.

O PLS n° 137, de 2000, de autoria do Senador Leomar Quintanilha, consiste em apenas um artigo, além da cláusula de vigência, e visa a aumentar em até o triplo as penas previstas para os crimes contra a pessoa, o patrimônio, a propriedade imaterial ou intelectual, os costumes, e a criança e o adolescente na hipótese de tais crimes serem cometidos por meio da utilização da tecnologia de informação e telecomunicações.

O PLS n° 76, de 2000, de autoria do Senador Renan Calheiros, apresenta tipificação de delitos cometidos com o uso de computadores, e lhes atribui as respectivas penas, sem entretanto alterar o Código Penal. Classifica os crimes cibernéticos em sete categorias: contra a inviolabilidade de dados e sua comunicação; contra a propriedade e o patrimônio; contra a honra e a vida privada; contra a vida e a integridade física das pessoas; contra o patrimônio fiscal; contra a moral pública e opção sexual, e contra a segurança nacional. Tramitou em conjunto com o PLS n° 137, de 2000, por força da aprovação do Requerimento n° 466, de 2000, de autoria do Senador Roberto Freire, por versarem sobre a mesma matéria.

O PLC n° 89, de 2003, de iniciativa do Deputado Luiz Piauhylino, altera o Decreto-Lei n° 2.848, de 7 de dezembro de 1941 (Código Penal), e a Lei n° 9.296, de 24 de julho de 1996, e dá outras providências. Resulta do trabalho do grupo de juristas que aperfeiçoou o PLC n° 1.713, de 1996, de autoria do Deputado Cássio Cunha Lima, arquivado em decorrência do término da legislatura. As alterações propostas visam a criar os seguintes tipos penais, cometidos contra sistemas de computador ou por meio de computador: acesso indevido a meio eletrônico (art. 154-A); manipulação indevida de informação eletrônica (art. 154-B); pornografia infantil (art. 218-A); difusão de vírus eletrônico (art. 163, § 3°); e falsificação de telefone celular ou meio de acesso a sistema informático (art. 298-A).

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

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

II – ANÁLISE

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

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

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

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

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

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

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

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

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

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

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

Vejamos cada um desses tipos.

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

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

Ademais, embora os três artigos possam ser reunidos em um só, preferimos manter a redação dada pelo PLC nº 89 de 2003, que define com maior clareza os delitos que se pretende tipificar. Entretanto propomos a alteração da pena original de detenção de 3 (três) meses a 1 (um) ano, e multa para detenção, de 1 (um) a 4 (quatro) anos, e multa, mantendo os mesmos parágrafos.

Ainda, quando este PLC nº 89 de 2003 estava sendo relatado nesta Comissão, o atento Senador Hélio Costa fez algumas sugestões de emendas que os membros da Comissão entenderam necessárias, mas que deveriam fazer parte de um novo Projeto de Lei a fim de que aquele projeto em discussão, uma vez aprovado, pudesse ir à sanção presidencial. Estando ele apensado ao PLS nº 76 de 2000 entendemos que é hora de acatar aqui algumas sugestões.

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

"Fraude Eletrônica

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

Pena – reclusão de dois a quatro anos e multa.

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

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

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

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

"Difusão Maliciosa de Código

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

Pena – reclusão de um a dois anos.

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

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

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

"Dispositivo de Comunicação e Sistema Informatizado

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

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

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

b) Arts. 163, §§ 2ºe 3º

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

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

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

“Dano por Difusão de Vírus Eletrônico

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

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

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

c) Art. 167 do CP

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

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

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

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

As alterações propostas para esses dispositivos são convenientes.

f) Arts. 298 e 298-A do CP

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

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

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

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

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

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

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

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

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

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

h) Art. 10 do PLC nº 89, de 2003

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

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

O PLS nº 76, de 2000, revestido de norma autônoma, afigura-se o projeto mais abrangente entre os que estão sendo aqui analisados. Os crimes informáticos estão divididos, no projeto, em crimes contra a inviolabilidade de dados e sua comunicação, contra a propriedade e o patrimônio, contra a honra e a vida privada, contra a vida e a integridade física das pessoas, contra o patrimônio fiscal, contra a moral pública e opção sexual e contra a segurança nacional.

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

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

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

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

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

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

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

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

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

b) Art. 1º, § 2º

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

c) Art. 1º, § 3º

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

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

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

d) Art. 1º, § 4º

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

e) Art. 1º, § 5º

As condutas descritas nos incisos I e II configuram crime contra a ordem tributária, definidos de forma mais abrangente e adequada nos arts. 1º e 2º da Lei nº 8.137, de 27 de dezembro de 1990.

f) Art. 1º, § 6º

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

g) Art. 1º, § 7º

Os crimes definidos nesse parágrafo já estão contemplados na Lei nº 7.170, de 14 de dezembro de 1983 (Lei de Segurança Nacional), especificamente nos seus arts. 13, 15 e 23.

Recentemente em Audiência Pública sobre o PLS nº 279 de 2003, do qual também sou relator, de autoria do nobre Senador Delcídio Amaral e que propõe a criação de um cadastro de titulares de correio eletrônico na internet, ficou evidente que, para fins de investigação, é necessário estabelecer um prazo legal de armazenamento dos dados de conexões e comunicações realizadas pelos equipamentos componentes da internet, o que será feito pelos seus provedores de acesso. Os serviços de telefonia e transmissão de dados mantêm por cinco anos os dados de conexões e chamadas realizadas por seus clientes para fins judiciais, mas na internet brasileira inexiste procedimento análogo.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

III – VOTO

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

SUBSTITUTIVO

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

Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal) e o Decreto-Lei nº 1.001, de 21 de outubro de 1969 (Código Penal Militar), para tipificar condutas realizadas mediante uso de rede de computadores ou internet, ou que sejam praticadas contra sistemas informatizados e similares, e dá outras providências.

O CONGRESSO NACIONAL decreta:

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

“Dano por Difusão de Vírus Eletrônico

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

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

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

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

“Capítulo VII-A

DA VIOLAÇÃO DE DISPOSITIVO DE COMUNICAÇÃO OU SISTEMA INFORMATIZADO

Acesso indevido a dispositivo de comunicação

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

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

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

§ 2º Somente se procede mediante representação, salvo se o crime é cometido contra a União, Estado, Município, empresa concessionária de

serviços públicos, agências, fundações, autarquias, empresas públicas ou sociedade de economia mista e suas subsidiárias.

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

Manipulação indevida de informação eletrônica

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

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

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

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

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

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

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

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

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

Divulgação de informações depositadas em banco de dados

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

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

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

Dados de conexões e comunicações realizadas

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

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

Permitir acesso por usuário não identificado e não autenticado

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

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

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

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

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

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

> **"Atentado contra a segurança de serviço de utilidade pública"**
>
> **Art. 265.** Atentar contra a segurança ou o funcionamento de serviço de água, luz, força, calor, informação ou telecomunicação, ou qualquer outro de utilidade pública:
>
> ..... (NR)"

> **"Interrupção ou perturbação de serviço telegráfico ou telefônico"**
>
> **Art. 266.** Interromper ou perturbar serviço telegráfico, radiotelegráfico, telefônico, telemático ou de telecomunicação, impedir ou dificultar-lhe o restabelecimento:
>
> ..... (NR)"

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

"**Difusão Maliciosa de Código**

> **Art. 266-A.** Difundir, por qualquer meio, programa, conjunto de instruções ou sistema informatizado com o propósito de induzir alguém a fornecer, espontaneamente e por qualquer meio, dados ou informações que facilitem ou permitam o acesso indevido ou sem autorização, a dispositivo de comunicação ou a sistema informatizado, ou a obtenção de qualquer vantagem ilícita:
>
> Pena – detenção de um a dois anos.
>
> Parágrafo único - A pena é aumentada de sexta parte, se o agente se vale de anonimato, de nome suposto ou da utilização de identidade de

terceiros para a prática de acesso.(NR)”

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

“**Art. 298.** .....

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

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

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

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

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

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

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

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

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

“Dano por Difusão de Vírus Eletrônico

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

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

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

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

“Capítulo VII-A

DA VIOLAÇÃO DE DISPOSITIVO DE COMUNICAÇÃO OU SISTEMA INFORMATIZADO

Acesso indevido a dispositivo de comunicação

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

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

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

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

Manipulação indevida de informação eletrônica

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

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

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

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

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

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

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

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

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

Divulgação de informações depositadas em banco de dados

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

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

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

Dados de conexões e comunicações realizadas

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

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

Permitir acesso por usuário não identificado e não autenticado

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

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

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

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

“Difusão Maliciosa de Código

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

Pena – detenção de um a dois anos.

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

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

“Capítulo VIII-A

DISPOSIÇÕES GERAIS

Art. 267-A. Equiparam-se à coisa o dado ou informação em meio eletrônico, a base de dados armazenada em dispositivo de comunicação e o

sistema informatizado, a senha ou qualquer meio que proporcione acesso aos mesmos.(NR)”

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

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

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

§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.

Sala da Comissão, em 20 de junho de 2006.

, Presidente

, Relator