O PROJETO DE LEI DOS CIBERCRIMES (PLS 76/2000): CRÍTICA AO SUBSTITUTIVO APROVADO NO SENADO

Vladimir Aras[1]

RESUMO

O presente artigo analisa o projeto de lei aprovado pelo Senado em julho de 2008, que tipifica certos cibercrimes e estabelece regras para a persecução desses delitos no Brasil.

PALAVRAS-CHAVE

Direito criminal brasileiro - Cibercrimes – Convenção de Budapeste (ETS 185) – Projeto de lei do Senado - Substitutivo

1. Introdução

Com o desenvolvimento das tecnologias da informação e, principalmente, com o advento da Internet, novas questões jurídicas surgiram, demandando respostas céleres do Estado, sob pena de o "tradicional" hiato existente entre o Direito e a realidade social vir a se tornar um enorme fosso, intransponível para os ordenamentos jurídicos nacionais.

Nesse contexto, discute-se a necessidade de uma legislação[2] penal e processual apta à proteção dos bens jurídicos da Sociedade da Informação. Aqui analisaremos alguns pontos do substitutivo do Senado aos projetos de lei n. 76/2000 e 89/2003, que tipifica crimes informáticos e examinaremos sua conformidade com a Constituição Federal, com o Código Penal e com o programa normativo da Convenção sobre Cibercriminalidade do Conselho da Europa (CoE)[3], também conhecida como Convenção de Budapeste ou ETS[4] 185. Este artigo é na verdade uma versão reduzida de ensaio que examina o substitutivo do Senado como um todo.

---

[1] Vladimir Aras, 38 anos, é mestre em Direito Público pela Universidade Federal de Pernambuco (UFPE), professor de processo penal do Centro Universitário Jorge Amado (Unijorge) e da Universidade Estadual de Feira de Santana (UEFS), professor de cursos de pós-graduação na Unifacs (BA), no JusPodivm (BA), na FTC-EAD (BA), no Verbo Jurídico (RS) e na Fase (SE), procurador da República na Bahia (MPF/BA), especializado em reforma processual penal latinoamericana pelo *Centro de Estudios de Justicia de las Americas* (CEJA), associado ao Instituto Brasileiro de Ciências Criminais (IBCCrim), membro da *International Association of Prosecutors* (IAP), professor do quadro da Escola Superior do Ministério Público da União (ESMPU), instrutor do Programa Nacional de Capacitação em Combate à Lavagem de Dinheiro (PNLD/MJ), membro do Grupo de Trabalho em Lavagem de Ativos da Procuradoria Geral da República (GT-LD), é um dos representantes do MPF no Grupo Operacional da Estratégia Nacional de Prevenção e Combate à Corrupção e à Lavagem de Ativos (ENCCLA), foi promotor de Justiça na Bahia (MP/BA) e integrou a força-tarefa do caso Banestado (MPF/PR). Email: vladimiraras@hotmail.com.

[2] ARAS, Vladimir. **Crimes de informática: uma nova criminalidade**. Jus Navigandi, Teresina, ano 5, n. 51, out. 2001. Disponível em: http://jus2.uol.com.br/doutrina/texto.asp?id=2250>. Acesso em: 01. jun. 2008.

[3] Vide www.coe.int.

[4] European Treaty Series.

2. Ameaças do ciberespaço: o crime de *phishing* e o estelionato eletrônico

Cada dia veem em maior número as notícias sobre cibercrimes, dos quais são espécies os delitos informáticos próprios (crimes praticados contra sistemas informáticos) e os delitos informáticos impróprios (crimes praticados por meio de sistemas informáticos). Na espécie "própria" ou "pura", reúnem-se práticas como o *hacking,* a difusão de *softwares* daninhos (*malware)* e os ataques de negação de serviço (*denial of service attacks*). Entre os delitos impróprios, estão os crimes de violação de direitos de autor, ciberpedofilia, ciberdiscriminação e estelionato informático.

A inexistência de uma legislação brasileira sobre cibercrimes *próprios* tem dificultado a persecução criminal de tais delitos. Embora a Internet comercial tenha sido implantada no Brasil em meados dos anos 1990, vários bens jurídicos penalmente relevantes ainda seguem desprotegidos. As violações mais sensíveis neste campo dão-se contra a confidencialidade, a integridade, a autenticidade e a disponibilidade de dados (informações) ou a funcionalidade de sistemas informáticos.

De outra banda, a falta de normas claras sobre os crimes de computador impróprios também produz controvérsias doutrinárias e jurisprudenciais, como a que se deu em torno da exata tipificação da subtração eletrônica de valores depositados com instituições financeiras. Esta conduta se perfaz pela clonagem de cartões por meio de copiadores ("chupa-cabras") ou pela obtenção de senhas mediante *phishing*, com engenharia social. O *phishing* é a fraude eletrônica, pela qual o agente obtém informações da vítima (senhas e dados pessoais), induzinda-a em erro, fazendo-se passar por terceiro (um banco ou um estabelecimento de *e-commerce*) ou levando o ofendido a confiar em arquivos informáticos infectados por softwares daninhos (*virus, worms* e *trojans*) que capturam ou copiam dados. A intenção do agente é a obtenção de vantagem patrimonial ilícita.

Ao examinar a questão da cópia de senhas bancárias para a obtenção de vantagem patrimonial ilícita, o STJ entendeu que esta conduta caracteriza crime de furto qualificado pela fraude, previsto no art. 155, §4º, inciso II, do Código Penal (pena de 2 a 8 anos de reclusão, e multa), afastando o enquadramento no art. 171 do Código Penal, pelo delito de estelionato (pena de reclusão de 1 a 5 anos, e multa).

A questão foi decidida no conflito negativo de competência 67.343/GO, o que por si só revela que a falta de dispositivos penais, mesmo nos casos de crimes informáticos impróprios, realmente pode tumultuar a persecução criminal. No caso concreto, divergia-se sobre o tipo penal incidente (se furto ou estelionato) e, por isso mesmo, não havia

consenso sobre a competência para a ação penal. Destaca-se: "*Conflito negativo de competência. Penal e processo penal. Fraude eletrônica na Internet. Transferência de numerário de conta da Caixa Econômica Federal. Furto mediante fraude que não se confunde com estelionato*" (CC 67343/GO, rel. ministra Laurita Vaz, 3ª Seção, j. 28.03.2007).

Uma das versões do substitutivo ao PLS 76/2000 pretendia tipificar o furto eletrônico no art. 155, §4º, inciso V do CP, com pena de reclusão de 2 a 8 anos e multa. Na mesma versão, o crime de estelionato eletrônico seria objeto do art. 171-A do CP, com o nome de "difusão de código malicioso". No entanto, o substitutivo aprovado no Senado em julho de 2008 abandonou o tratamento do tema em duas figuras distintas. Agora, conforme o substitutivo, o estelionato informático (*phishing)* será tipificado no inciso VII do §2º do art. 171 do CP, e não se cuidará do furto eletrônico, crime informático impróprio perfeitamente enquadrável aos esquemas típicos das formas qualificadas de furto, seja com fraude ou mediante destreza.

Por outro lado, colocou-se o crime de estelionato com *phishing* no lugar devido, o que permitiu adequar sua pena ao padrão normativo do Código Penal, já que na proposta anterior a sanção era de 1 a 3 anos. Assim, andou melhor o legislador ao manter a estrutura do estelionato simples (art. 171 do CP), prevendo no inciso VII do §2º do art. 171 outro meio fraudulento de obtenção de vantagem ilícita, em prejuízo alheio, tendo como agente quem "*difunde, por qualquer meio, código malicioso com intuito de facilitar ou permitir acesso indevido à rede de computadores, dispositivo de comunicação ou sistema informatizado*". Cria-se então o "estelionato eletrônico".

Embora tenha descartado a tipificação do furto eletrônico, a proposta contém, todavia, três equívocos. O primeiro está no inciso VII do §2º do art. 171 do CP, o qual não exige que o "código malicioso"[5] seja executado para que o crime se consume. Segundo o dispositivo bastaria a difusão, por qualquer meio, do *malware*, com o objetivo de obter acesso indevido a sistema informático. Tal redação não é suficientemente clara. Parece evidente que somente poderá haver estelionato, se o programa de computador destinado à obtenção da vantagem ilícita for executado em um determinado sistema informático. Sem o acionamento da rotina programada para a cópia de dados, ou pelo menos sem a tentativa de execução, não se poderá obter vantagem indevida em prejuízo alheio. A simples difusão do *malware* pode caracterizar outro crime, mas não o estelionato.

[5] Péssimo anglicismo, derivado da contração das palavras *malicious software*. É sinônimo de *software* daninho, englobando *vírus, worms e trojans*.

O segundo problema. O art. 171-A, sugerido na versão anterior do substitutivo, era silente sobre a aplicabilidade da causa especial de aumento de pena prevista no atual art. 171, §3º do CP, que pune mais severamente o crime de estelionato cometido contra entidade de direito público[6]. Agora, o substitutivo aprovado pelo Senado em 10 de julho de 2008 continua silenciando sobre esse ponto e, pior, revoga tacitamente a referida majorante. Isto porque no projeto está previsto um novo §3º com a seguinte redação: "*Se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática do crime do inciso VII do §2º deste artigo, a pena é aumentada de sexta parte*". Como se trata de simples falha de numeração, o novo §3º deve ser reposicionado, passando a ser o §4º do art. 171 do CP, com o que estará mantida a estrutura atual do crime de estelionato, com suas formas equiparadas e a necessária majorante.

O terceiro equívoco, na verdade uma omissão, é mais grave do que os anteriores. É que, diferentemente dos demais incisos do art. 171, §2º do CP, o novo inciso VII (estelionato eletrônico) não deixa claros dois elementos indispensáveis a este delito: a intenção de lucro e o ânimo de causar prejuízo a outrem. Em outras palavras, todas as formas equiparadas previstas no §2º do art. 171 do CP apresentam elementos normativos específicos, nos quais é possível identificar, de pronto, que se exige a intenção do agente de auferir vantagem ilícita mediante a causação de prejuízo a outrem. Isto não se passa com o futuro inciso VII, na redação que lhe foi dada pelo Senado. Com isso, cria-se um novo problema, um conflito entre o art. 171, §2º, VII, do CP (estelionato eletrônico) e o art. 163-A, §1º, do CP (inserção ou difusão de código malicioso seguida de dano), novos delitos com estrutura típico-normativa semelhante[7], especialmente no que diz respeito à intenção, em ambos, de obter acesso indevido a sistema informático.

A obtenção de vantagem para a configuração do estelionato sempre foi da tradição do direito penal brasileiro. A Lei 2.033, de 20 de setembro de 1871, assim dispunha no seu artigo 21: "*Em geral o estellionato, de que trata o § 4º do art. 264 do Código Criminal, é o artifício fraudulento, pelo qual se obtenha de outrem a entrega de dinheiro, fundos, títulos ou quaesquer bens, pelos seguintes meios: §1º Usando-se de falso nome ou falsa qualidade; §2º Usando-se de papel falso ou falsificado*".

---

[6] "§3º. A pena aumenta-se de um terço, se o crime é cometido em detrimento de entidade de direito público ou de instituto de economia popular, assistência social ou beneficência".

[7] "Art. 163. Inserir ou difundir código malicioso em dispositivo de comunicação, rede de computadores ou sistema informatizado".

No direito comparado, é de se ver que o Código Penal português[8] desconhece o crime de furto eletrônico. O art. 221, inciso 1, do CP lusitano cuida do crime de burla informática (estelionato), punindo-o com pena de prisão de até 3 anos ou multa. Se o prejuízo for de valor elevado a pena pode alcançar 8 anos de prisão.

Na Espanha, o legislador também preferiu tipificar o estelionato eletrônico, deixando de lado o furto. O art. 248, n. 2, do Código Penal espanhol[9] assim descreve a *estafa informática*: "*2.- También se consideran reos de estafa los que, con ánimo de lucro, y valiéndose de alguna manipulación informática o artificio semejante consigan la transferencia no consentida de cualquier activo patrimonial en perjuicio de tercero*". A mesma pena se aplicará ao agente que fabricar, introduzir, possuir ou fornecer *softwares* especificamente destinados à prática de estelionato. As penas vão de 6 meses a 6 anos, nas formas simples e qualificada.

Cezar Bittencourt explica que "*Para a configuração do estelionato é indispensável que o agente obtenha proveito indevido em prejuízo alheio. Exige o tipo penal a produção do duplo resultado*"[10.] Portanto, é preciso alterar a redação do inciso VII do §2º do art. 171 do CP, de modo que fique expresso que a difusão do *malware* tem como finalidade última a obtenção de vantagem ilícita em prejuízo alheio[11.] Para isto, pode-se aproveitar a experiência espanhola ou lusitana, ou seguir o esquema do art. 8º da Convenção de Budapeste, e aperfeiçoar a redação do tipo penal de estelionato eletrônico, adequando-o à realidade brasileira.

Com efeito, o art. 8º da Convenção de Budapeste determina que cada Estado-Parte tipifique a ação dolosa de causar prejuízo a outrem, mediante a introdução, alteração, eliminação ou supressão de dados informáticos, ou por meio de qualquer intervenção no funcionamento de um sistema informático. Exige-se sempre que o agente tenha a intenção de "*obter um benefício econômico ilegítimo para si ou para terceiros.*"

Em função do modelo da Convenção dos Cibercrimes, propomos a seguinte redação para o inciso VII do §2º do art. 171 do CP:

> "Art. 171. [...]
> §2º. Nas mesmas penas incorre quem:

---

[8] Vide o texto do Código Penal da República Portuguesa. Disponível em: http://www.unifr.ch/ddp1/derechopenal/legislacion/pt/CPPortugal.pdf. Acesso em: 31.maio.2008.

[9] Disponível em www.delitosinformaticos.com. Acesso em: 31.maio.2008.

[10] BITTENCOURT, Cezar Roberto. **Tratado de direito penal: parte especial: v. 3**. São Paulo: Saraiva, 2003, p.280.

[11] *Mutatis mutandi*, as observações aqui postas também servem à disciplina do crime militar de estelionato eletrônico, que corresponderá ao art. 251, §1º, inciso VI, do CPM.

> VII – introduz, altera, elimina ou suprime dados informáticos ou, de qualquer modo, intervém no funcionamento de um dispositivo de comunicação, rede de computadores ou sistema informático, para obter vantagem ilícita para si ou para outrem, em prejuízo alheio.
> §3º. [...]
> §4º. Se o agente usa nome falso ou dados pessoais de terceiros, ou abusa do anonimato, a pena é aumentada de sexta parte."

3. O crime de acesso não autorizado a sistema informático (*hacking*)

O crime de acesso indevido ou ilegítimo a sistemas computacionais, ou *hacking*, é objeto do art. 285-A do PLS 76/2000. O tipo encabeça o novo capítulo IV do título VIII, que cuidará dos "crimes contra a segurança dos sistemas informatizados". A Convenção de Budapeste adota a expressão "sistema informático", como se vê no seu art. 1º, letra 'a'. A Lei Portuguesa 109/91 (Lei da Criminalidade Informática) também se vale da expressão "sistema informático", definida em seu art. 2º, 'b'. Em oportunidade anterior, ao cuidar de crimes de computador, o legislador brasileiro adotou a forma "sistemas de informações", também criticável. É o que se passa com os tipos do art. 153, §1º-A, do art. 313-A e do art. 313-B do CP, resultantes da Lei 9.983/2000. Parece-nos adequado acompanhar a redação da Convenção de Budapeste, mediante a substituição do adjetivo "informatizado" por "informático"[12].

O novo crime do art. 285-A do CP será um dos delitos contra a incolumidade pública, e se consumará quando o agente acessar rede de computadores, dispositivo de comunicação ou sistema informático protegidos por restrição de acesso. Vale dizer: punir-se-á o simples acesso a sistema informático, englobando redes governamentais ou particulares (corporativas ou não), que sejam privadas ou de acesso restrito, desde que haja medidas de segurança computacionais ativas, destinadas a impedir o acesso ilegítimo ou não autorizado, a exemplo de senhas, criptografia, segurança biométrica, *firewalls*, etc. Este é o exato sentido de "expressa restrição de acesso", que se deve interpretar em conjunto com o requisito de "violação de segurança".

Logo, a restrição de acesso não diz respeito à violação de direitos autorais, ou a violação de termos de uso de um site. O que se tem em mira é o rompimento de medidas de segurança tecnológicas implantadas para impedir o acesso ilegítimo ao próprio sistema informático pertencente a terceiro. Não se tem em vista proteger a propriedade intelectual, objeto de outros tipos penais (art. 184 do CP e Lei n. 9.609/98). Assim, mesmo nos casos de

[12] Complicando esse cenário, o art. 72 da Lei Federal 9.504/97 utiliza a forma "sistema de tratamento automático de dados".

desbloqueio de celulares, tocadores de DVD, consoles de videogames, ou *gadgets* não haverá o crime, uma vez que o agente não estará acessando rede ou dispositivo de terceiro. Também não ocorrerá o crime com a simples utilização de conteúdo publicado em sites da Internet em blogs ou em *mashups*[13].

A pena do crime do art. 285-A do CP será de 1 a 3 anos de reclusão, e multa, salvo na forma prevista no parágrafo único, hipótese na qual a pena deverá ser aumentada de um sexto. É o que ocorre se o agente "*se vale de nome falso ou da utilização de identidade de terceiros*" (sic). Em relação ao parágrafo único do art. 285-A cabe uma primeira sugestão. Poderia o legislador expressar o preceito de forma mais simples, mais abrangente e mais direta: "*Se o agente usa nome falso ou dados pessoais de terceiros, ou abusa do anonimato, a pena é aumentada de sexta parte*". De qualquer modo, haverá dificuldades de interpretação desse parágrafo, já que o elemento "nome falso" pode confundir-se com o *nickname* (apelido) ou com o *avatar* (personalidade virtual) que o agente utilize em suas relações usuais no ciberespaço. Cumprirá à doutrina e à jurisprudência precisar o conceito de "nome falso" nas relações virtuais.

Apesar de tais dificuldades, o art. 285-A do CP estará em consonância com o art. 2º da Convenção de Budapeste, que tipifica como crime o acesso intencional (doloso) e ilegítimo à totalidade ou a uma parte de um sistema informático. Para reduzir o espectro punitivo dessa infração, o tratado faculta às Partes exigir, para a configuração do delito, que haja violação de medidas de segurança, ou que o agente tenha a intenção de obter dados informáticos de terceiros ou tenha outra intenção ilegítima.

No mesmo novo capítulo IV do Título VIII do Código Penal, o substitutivo aprovado no Senado cuida do crime de "obtenção, transferência ou fornecimento não autorizado de dado ou informação", objeto do futuro art. 285-B do Código Penal, conforme a proposta. Em redação sofrível e confusa, tal artigo veicula um novo tipo penal, aparentemente distinto do crime do art. 285-A (acesso não autorizado), segundo o qual passará a ser crime "*obter ou transferir, sem autorização ou em desconformidade com autorização do legítimo titular da rede de computadores, dispositivo de comunicação ou sistema informatizado, protegidos por expressa restrição de acesso, dado ou informação neles disponível*".

A pena do crime do art. 285-B será a mesma da forma básica de *hacking*, a ser prevista no art. 285-A do CP, isto é, reclusão, de 1 a 3 anos, e multa. O parágrafo único

[13] Aplicação web que utiliza dados de fontes diversas, combinando-os numa ferramenta integrada. Exemplo: sites que integram o serviço GoogleMaps para facilitar a localização de endereços que indicam.

contém causa especial de aumento de pena: se o dado (ou informação) obtido for fornecido a terceiros, a pena é aumentada de um terço.

A redação imperfeita pode conduzir a confusão interpretativa, como se o art. 285-B se destinasse a proteger os direitos autorais. Não se trata de punir o intercâmbio de informações na Internet nem de tolher a criatividade ou o livre fluxo de idéias. O tipo não se dirige a proibir condutas do tipo *peer-to-peer* (P2P), compartilhamento via *BitTorrent* ou *LimeWire*, nem quer impedir a troca de arquivos de MP3, nem pretende obstar o acesso a redes informáticas abertas (*wi-fi*), porque nesses casos o acesso é legítimo e consentido pelos usuários da rede de compartilhamento, ou pelo mantenedor da rede *wi-fi*, ou há a anuência de quem disponibilizou o conteúdo não protegido. Frise-se, todavia, que a obtenção indevida de dados protegidos por *copyright* continua sendo crime, porque tais condutas estão tipificadas como violação de direitos autorais (art. 184 do CP). Enfim, o novo art. 285-B do CP punirá o *hacking*, a invasão de sistemas informáticos, e não qualquer forma de obtenção de informações na Internet. A punição por esse crime decorrerá do acesso indevido a um sistema informático, e não da violação de direito de autor.

Além do que já apontamos, há outros três problemas patentes no art. 285-B do CP. O primeiro está no objeto material da infração, que é o dado ou a informação. O projeto não define "dado". O art. 16, incisos V e VI, do substitutivo traz definições para "dado informático" e "dados de tráfego". É a esses dados, especialmente a primeira espécie, a que o tipo se refere? Caso a resposta seja positiva, o legislador deveria ter utilizado a expressão completa, "dado informático", abandonando, em consequência, a palavra "informação". Isto, porque o bem jurídico "informação" já fará parte do conceito legal de dado informático, conforme o inciso V do art. 16: "*qualquer representação de fatos, de informações ou de conceitos, sob forma suscetível de processamento numa rede de computadores ou dispositivo de comunicação ou sistema informatizado*".

A segunda dificuldade revela-se ao cotejar o art. 285-B do CP com a parte final do art. 2º do ETS 185. Na verdade, o crime de "*obtenção, transferência ou fornecimento não autorizado de dado ou informação*" deveria ser uma forma qualificada do delito de acesso ilegítimo, este previsto no art. 285-A. No entanto, o legislador optou por criminalizar essa conduta em outro tipo, supostamente autônomo, e, pior, atribuiu-lhe a mesma pena da forma básica de *hacking*, embora a ação descrita no art. 285-B seja evidentemente de maior reprovabilidade penal. Afinal, no art. 285-B, o agente não se satisfaz com o acesso indevido; ele também obtém dados ou informações (*rectius*: dados informáticos) disponíveis no sistema

computacional, e, por isso mesmo, lesa mais gravemente os interesses do legítimo detentor ou do titular de tais dados.

Portanto, não faz sentido a separação da conduta em dois tipos, pois que, para obter ou transmitir o dado, como exige o art. 285-B, é imprescindível o acesso ilegítimo (desautorizado ou para além da autorização concedida), tipificado no art. 285-A, sempre mediante a violação de medidas de segurança que afastem a restrição de acesso. Consequentemente, se a conduta "B" é mais grave do que a conduta "A", também não é correta a escala penal proposta para o novo art. 285-B. Sem dúvida, esta deve ser mais severa. Observe-se, ainda uma vez, que o art. 2º da Convenção de Budapeste especifica que o crime de acesso ilegítimo pode ter como elemento subjetivo do injusto "a intenção de obter dados informáticos" e isto, definitivamente, é mais reprovável do que simplesmente acessar indevidamente um sistema computacional, mas sem obter ou pôr a descoberto informações alheias.

O terceiro problema na redação do art. 285-B está na incompatibilidade entre o crime do *caput* e a forma agravada do seu parágrafo único, que trata do "fornecimento" a terceiros de dado ou informação (*rectius*: dado informático) obtido sem autorização. Não é possível conciliar tal descrição normativa com a conduta típica de "transferir" dado informático, prevista no caput do mesmo artigo 285-B. De fato, se o agente transfere dado (*caput*) que obteve indevidamente estará necessariamente fornecendo-o a terceiro (parágrafo único). Para quem mais transferiria os dados, senão a outrem? Destarte, tal redação é ilógica e não pode ser mantida, porque foram previstas penas distintas para condutas semelhantes.

O certo é que, nos três casos (obter, transferir e fornecer), o que se procura tutelar é a confidencialidade da informação, isto é, o sigilo do dado informático[14]. Então, essas três condutas são igualmente reprováveis. Além disso, é necessário fazer incluir o intuito de lucro como causa especial de aumento de pena, ao lado do uso de nome falso ou de identidade alheia (parágrafo único). Quanto aos dados pessoais em si mesmos, estes deverão ser tutelados no art. 154-A, objeto do substitutivo.

Enfim, para solucionar as falhas do art. 285-B, sugerimos as seguintes alterações, que implicam a reformulação da redação do art. 285-A:

> Art. 285-A. Acessar, sem autorização do legítimo titular, quando exigida, ou mediante violação de segurança, rede de computadores, dispositivo de comunicação ou sistema informático, protegidos por restrição de acesso:

[14] E não sua integridade ou sua disponibilidade, porque aí o crime seria outro (dano eletrônico).

> Pena – reclusão, de 1 (um) a 3 (três) anos, e multa.
>
> §1º. Se, mediante o acesso não autorizado, o agente obtém, para si ou para outrem, revela, fornece ou transfere a terceiro dado informático disponível em rede de computadores, dispositivo de comunicação ou sistema informático, a pena é de reclusão, de 2 (dois) a 4 (quatro) anos, e multa.
>
> §2º. Se o agente usa nome falso ou dados pessoais de terceiros, ou abusa do anonimato[15], ou se o crime é praticado com o fim de lucro, a pena é aumentada de sexta parte.
>
> §3º. Somente se procede mediante representação, salvo se o crime é cometido contra a União, Estado, Município, o Distrito Federal, empresa concessionária de serviços públicos, fundação, autarquia, empresa pública ou sociedade de economia mista ou sua subsidiária.

Como se vê, como consequência da supressão do art. 285-B, o art. 285-C, que cuida da modalidade de ação penal (pública condicionada à representação), passaria a ser um parágrafo do art. 285-A, acrescentando-se entre os entes públicos o Distrito Federal, que ali não estava, e suprimindo-se a menção a agências em função da redundância, pois a natureza jurídica destas é de autarquia. A alteração terá a vantagem de deixar claro que o que se busca punir não é a obtenção de informações em redes ou sistemas informáticos, mas sim a obtenção de tais dados mediante acesso ilegítimo (*hacking*). Portanto, o acesso regular a sistemas P2P e a redes *wi-fi* continua sendo fatos atípicos, quando não se verificar a prática de violação de direitos autorais (art. 184 do CP).

4. Prazo de guarda ou custódia dos dados de tráfego

O art. 22 do substitutivo impõe ao "*responsável pelo provimento de acesso a rede computadores*" uma série de obrigações. Antes de examiná-las, é necessário apontar a falha de redação do *caput*, que só se refere aos provedores de acesso, deixando de regular as obrigações legais dos provedores de hospedagem, de modo que o objetivo da Lei dos Cibercrimes pode-se ver frustrado nos casos em que os dados necessários à persecução não estejam à disposição do provedor de acesso (o fornecedor da conexão à Internet), mas sim a cargo de outras espécies de provedores, isto é, do mantenedor do site no qual está postado ou publicado o conteúdo ilícito, ou no qual se consumou a conduta criminosa.

Avançando no exame do art. 22 do substitutivo vemos que o inciso I estabelece prazo de 3 anos para guarda de dados de tráfego (*logs* de conexão). Em uma de suas versões primitivas, o projeto previa guarda por 5 anos. Observe-se que alguns dos crimes objetos do substitutivo ou previstos noutros diplomas terão penas superiores a 4 anos de

[15] Há programas informáticos e serviços on-line que permitem ocultar a identidade do atacante. São os *anonymizers* e os *anonymous remailers.*

reclusão. É o caso do art. 171, §2º, VI; do art. 163-A, §§1º e 2º; do art. 265; do art. 297 e do art. 298, do CP e do art. 241 do ECA. Em todas essas situações, a prescrição da pretensão punitiva em abstrato ocorrerá em 12 anos, pela regra do art. 109, inciso III, do CP. Todavia, para qualquer delito, inclusive os ora mencionados, será de somente três anos o prazo de guarda dos dados de conexão, informação essencial ao rastreamento de cibercrimes e à determinação da autoria.

Compreende-se que o armazenamento de dados exige grande dispêndio de recursos por provedores e empresas de telecomunicações. Afinal, deverão ser preservados os dados de todas as conexões realizadas pelo usuário (dados de tráfego, e não dados de conteúdo). Por isso mesmo, houve grande reação de entidades representativas de provedores contra tal dispositivo[16]. Movimento semelhante se viu durante os trabalhos preparatórios da Convenção de Budapeste, que prevê prazo de guarda mínimo de 90 dias, prorrogáveis (art. 16, n. 2, do ETS 185).

Na verdade, conforme o projeto, os provedores têm duas obrigações distintas, a manutenção dos dados de tráfego por até 3 anos (art. 22, inciso I, do substitutivo); e a preservação imediata de outros dados úteis à persecução criminal (art. 22, inciso II).

No primeiro caso, o provedor deve preservar os dados de tráfego (e somente estes) por até 3 anos, sem previsão de prorrogação e independentemente de ordem judicial. No segundo caso, o provedor, apenas mediante requisição judicial, deve preservar outras informações (inclusive o conteúdo de comunicações armazenadas, dados cadastrais e outros elementos probatórios) por um prazo a ser estabelecido pela autoridade judicial requisitante. Em regra, esse prazo deve ser o necessário para a cópia dos dados e a realização de perícia de computação forense.

No entanto, haverá situações nas quais a guarda dos dados de conexão não permitirá rastrear o autor do ilícito. Isto ocorrerá quando o agente utilizar computadores em *lan houses* ou cibercafés ou conectar-se à Internet em redes *wi-fi* públicas, como as existentes em shoppings e em algumas cidades *digitais*. Assim, a identificação do autor do ilícito dependerá de outros instrumentos de investigação, como vídeos de câmeras de segurança, dados de cartões de crédito, ou da realização de vigilância da pessoa investigada.

De qualquer modo, se não prevalecer a proposta do Senado, a persecução criminal poderá restar inviabilizada em grande número de crimes, embora não prescrita a ação penal, simplesmente porque não será possível elucidar a autoria, problema crucial da

---

[16] "*Prazo para guardar de logs de internet deve ser modificado, diz Abranet*". Disponível em: http://idgnow.uol.com.br. Acesso em 20.jul. 2008.

cibercriminalidade. Portanto, está nas mãos da Câmara dos Deputados a tarefa de assegurar ao Ministério Público e à Polícia, assim como às vítimas, tempo suficiente para que, ao longo de uma investigação, seja possível obter os dados necessários à identificação de ciberdelinquentes.

5. O polêmico art. 22 do substitutivo do Senado

Conforme o art. 16, inciso VI, do PLS 76/2000, dados de tráfego são "*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 tipo do serviço subjacente*". São eles uma das espécies dos dados informáticos (inciso V). O conceito está em conformidade com a Convenção de Budapeste.

A partir desse dispositivo, percebem-se algumas outras deficiências do art. 22 do projeto do Senado, além da já descrita no item 4, acima.

A primeira. No inciso I do art. 22 adota-se erroneamente o conceito de tempo GMT (*Greenwich Mean Time)*, que, por ter conotação geográfica, foi substituído pelo especificação *UTC – Universal Time, Coordinated* (Tempo Universal Coordenado), que é uma medida derivada do Tempo Atômico Internacional.

A segunda. O art. 22, inciso I, não utilizou a definição de dados de tráfego instituída pelo próprio substitutivo no art. 16, inciso VI. De fato, o legislador diz que cabe ao provedor de acesso preservar "*os dados de endereçamento eletrônico da origem, hora, data e a referência GMT da conexão efetuada por meio de rede de computadores e por esta gerados*", quando bastaria dizer que o provedor deve preservar os dados de tráfego e fornecê-los quando solicitados.

A terceira. Ao utilizar as expressões "*objetivo de provimento de investigação pública formalizada*"[17] e "*cujo fornecimento será feito exclusivamente à autoridade investigatória*", o art. 22, inciso I, do substitutivo exclui de seu rol o querelante, que é autor de ação penal privada e não é "autoridade investigatória", e impede o acesso aos dados de tráfego em causas cíveis não-públicas ("investigação pública formalizada"), como as propostas por pessoas físicas e jurídicas para a tutela da honra, da intimidade, da imagem e da vida privada (art. 5º, incisos IV e V, da Constituição).

[17] Expressão que, por si só, merece crítica, por não seguir a melhor técnica de redação jurídica.

Há uma quarta deficiência. O inciso II do art. 22 do projeto levanta óbice à eficiência e à rapidez da persecução cibercriminal, pois exige "*requisição judicial*" para um simples pedido de preservação de dados de tráfego ou de outras informações necessárias à investigação.

Em outras legislações, como a norte-americana (*18 U.S.C. §2703*) e a holandesa (*Vorderen Gegevens Telecommunicatie)*, o Ministério Público pode requisitar por si mesmo a conservação de dados de conexão, ou aceder diretamente aos dados de tráfego e a informações cadastrais dos usuários de sistemas informáticos públicos. O art. 15, n. 2, da Convenção de Budapeste, permite que as medidas processuais nela mencionadas sejam concretizadas mediante controle judicial ou "outras formas de controle independente", com indicação dos fundamentos que justificam sua aplicação. Entre essas outras formas de controle está, sem dúvida, a atuação do Ministério Público, mediante requisição, para instrução de procedimentos criminais ou de inquéritos civis sob sua presidência.

Não há razão para se exigir tutela judicial para a mera conservação de dados (sejam de tráfego ou de conteúdo), já que o Ministério Público e a Polícia requisitarão apenas a preservação dos dados, para permitir seu conhecimento posterior, mediante decisão judicial. A propósito, há contradição entre os incisos I e II e o inciso III do art. 22 do PLS, pois este permite aos provedores, sem prévia autorização judicial, que informem "à autoridade competente" (Ministério Público e Polícia Judiciária) suspeita de crime de ação penal pública que tenha sido cometido na "rede de computadores sob sua responsabilidade". Trata-se da boa e velha *notitia criminis*, que pode, e aqui deve, ser apresentada pelos provedores. Mas, contraditoriamente, se, diante da inércia do provedor, o Ministério Público e a Polícia necessitarem desses mesmos dados, deverão apresentar requerimento à autoridade judicial, para que deles tomem conhecimento.

A quinta deficiência. O inciso II do art. 22 do projeto nada diz sobre o prazo de conservação dos dados após a ordem judicial de preservação. À primeira vista, este prazo deveria ser equivalente ao do inciso I, que é de três anos. Mas, se bem observado o problema, ver-se-á que a conservação "de outras informações" necessárias à investigação deve perdurar por prazo razoável, até a coleta oficial de tais dados, de modo a permitir o pleno contraditório, com as perícias e contraperícias que se mostrarem úteis.

O sexto problema. O inciso III do mesmo art. 22 incorre em outros equívocos, ao utilizar a palavra "denúncia" em seu sentido vulgar, em lugar de "notícia-crime", e "crime sujeito a acionamento penal público incondicionado" em vez de "crime de

ação penal pública". Em direito processual penal, denúncia tem sentido unívoco e é a peça inicial da ação penal pública.

A sétima deficiência. No §2º do mesmo art. 22 prevê-se a aplicação de sanção pecuniária a provedores de acesso, mediante procedimento de feição administrativa, conduzido pela autoridade "judicial" desatendida. Esta não é a melhor solução para o desatendimento a ordens judiciais, não havendo dispositivo semelhante na legislação penal[18]. Além disso, haveria uma superposição de infrações. É que o Código Penal conhece o crime de desobediência com pena de detenção, de 15 dias a 6 meses, e multa. Haveria então duas multas: a penal e a administrativa.

É de se ver, outrossim, que, além da resposta penal, a legislação já permite a medida cautelar de busca e apreensão e a propositura de ação civil pública para situações de reiterado descumprimento de ordens judiciais. A existência de outro processo (administrativo) perante a autoridade judicial desatendida trará prejuízo à própria persecução criminal, em virtude da divisão de esforços entre a instrução processual penal e a apuração dessa outra infração praticada pelo provedor. Pelo que se vê, não convém que se inove neste ponto. Solução intermediária seria a de atribuir ao órgão mencionado no §1º do art. 22 do PLS a função de aplicar as multas previstas no §2º, mediante processo administrativo. Sugere-se que este órgão seja a Agência Nacional de Telecomunicações (Anatel) ou o Instituto Nacional de Tecnologia da Informação (ITI).

Ainda temos outras objeções à redação do §2º do art. 22 do PLS. Conforme o referido parágrafo, a multa decorreria do descumprimento de requisições judiciais para o fornecimento de dados de tráfego ou outros dados informáticos. No entanto, o projeto não prevê a mesma sanção para o caso de desatendimento direto do dever de guarda dos dados de tráfego, nem para a devassa dos dados referidos no inciso II do art. 22, em caso de quebra de "confidencialidade e inviolabilidade". Por falta de previsão expressão, a multa do §2º também não se aplicaria em caso de descumprimento do dever de informar previsto no inciso III (notícia-crime), muito menos ao caso de recusa a submeter-se a auditoria mencionada no §1º.

6. "Vigilantismo" ou dever de colaboração?

O art. 22, inciso III, do projeto aprovado pelo Senado tem merecido severa oposição de usuários, internautas e ongues, sob a crença de que estimulará injustiças na Internet e transformará provedores em fiscais de seus clientes. O dispositivo exige do

[18] Por exemplo, as infrações não-penais (administrativas) previstas no ECA estão sujeitas a multa, aplicada pelo Juiz da Infância e da Adolescência, em procedimento autônomo.

provedor que informe "*de maneira sigilosa, à autoridade competente, denúncia que tenha recebido e que contenha indícios da prática de crime sujeito a acionamento penal público incondicionado, cuja perpetração haja ocorrido no âmbito da rede de computadores sob sua responsabilidade."*

Malgrado sua sofrível redação, o inciso III do art. 22 do projeto é útil e não tem por objetivo promover o denuncismo descontrolado ou o *vigilantismo* virtual. Aliás, dispositivo desta ordem não é novidade. É da tradição brasileira a existência da obrigação legal de comunicar a ocorrência de crimes. Por exemplo, o art. 66 da Lei das Contravenções Penais (Decreto-lei n. 3.688/41) considera infração punível com multa "*deixar de comunicar à autoridade competente crime de ação pública, de que teve conhecimento no exercício de medicina ou de outra profissão sanitária, desde que a ação penal não depende de representação e a comunicação não exponha o cliente a procedimento criminal*". O mesmo se passa com o art. 245 da Lei n. 8.069/90.

Assim, a *ratio essendi* do referido inciso III está ligada à prevenção de atos gravemente lesivos ao interesse social, como a ciberpedofilia e práticas ilícitas de *phishing*. Não se trata de instrumentalizar a proteção a direitos autorais. Observe-se que os provedores só estarão obrigados a noticiar à Polícia ou ao Ministério Público crimes de ação penal pública. A maior preocupação das entidades que defendem a liberdade na Internet está no suposto prejuízo que tal inciso poderia trazer para os usuários de redes de compartilhamento de arquivos do tipo *peer-to-peer* (P2P). Os crimes contra a propriedade intelectual, vulgarmente chamados de "pirataria", não são objeto da nova Lei dos Cibercrimes, pois estão previstos no art. 184 e §§1º a 4º do Código Penal. A forma do *caput* é de ação penal privada, sujeita a queixa-crime e consiste em "*violar direitos de autor e os que lhe são conexos*". O crime de violação de direitos de autor será de ação penal pública incondicionada nas formas previstas nos §§1º e 2º do art. 184, nas quais há intuito de lucro. A forma do §3º é de ação penal pública *condicionada* à representação.

Por conseguinte, não haverá vigilância indiscriminada sobre todo tipo de conteúdo que circula na Internet. Esse temor é infundado. As comunicações telemáticas continuarão protegidas na forma do art. 5º, incisos X e XII, da Constituição e da Lei 9.296/96, somente podendo ser afastada a sua inviolabilidade mediante autorização judicial, a pedido do Ministério Público ou da Polícia, para a instrução de investigação criminal ou processo penal. O provedor não estará autorizado a vasculhar comunicações "fechadas", criptografadas ou não, nem poderá devassar o conteúdo das informações que trafegam por seus servidores, sob

pena de seus administradores praticarem o crime do art. 10 da Lei 9.296/96 ou os delitos dos arts. 153 e 154 do CP.

Somente se um provedor identificar, por meios próprios em conteúdos abertos, ou por informação de terceiro, a prática de crimes de ação penal pública, como pedofilia cibernética ou estelionato eletrônico cometidos em seus servidores, é que estará obrigado a expedir *notitia criminis* na forma do art. 22, inciso III, do projeto do Senado. O mesmo se dará se a empresa identificar violação de direitos de autor com o fim de lucro (§§1º e 2º do art. 184 do CP). No entanto, se verificar o crime de violação de direitos autorais na forma simples, sem intuito lucrativo ou finalidade comercial (art. 184, *caput*), ou na forma do §3º (trocas de obras protegidas em redes sociais ou em redes de compartilhamento de conteúdo), o provedor não estará obrigado a comunicar o suposto crime, porque estes delitos não são de ação penal pública *incondicionada*, por força do que dispõe o art. 186, incisos I e IV, do Código Penal[19].

Não é necessário que o legislador arrole os crimes em que deve haver o oferecimento de notícia-crime por parte dos provedores. Isso fugiria à melhor técnica legislativa. Basta que o dispositivo contenha, como fez o legislador, referência ao gênero de delitos em que essa comunicação formal deve ocorrer.

Frise-se que o dever de colaboração decorre do direito fundamental à segurança, previsto no art. 5º e no art. 144 da Constituição. Afinal, segundo este último dispositivo a segurança pública é dever do Estado, direito e responsabilidade de todos.

7. Alteração da Lei da Repressão Uniforme

O art. 21 do substitutivo ao PLS 76/2000 pretende alterar a Lei da Repressão Uniforme (Lei 10.446/2002), para permitir a atuação da Polícia Federal na investigação de delitos "*praticados contra ou mediante rede de computadores, dispositivo de comunicação ou sistema informatizado*" (inciso V). O dispositivo renderá controvérsias e poderá inviabilizar outras atividades da Polícia Federal, já que, pela regra, todo e qualquer crime informático (próprio ou impróprio) poderá ser investigado pela polícia judiciária da União. Não nos parece adequada essa previsão. A Polícia Federal não terá estrutura para apurar adequadamente toda a enorme gama de delitos que se encaixam nesse paradigma. Os já escassos recursos da Polícia Federal devem ser destinados à investigação de crimes federais por excelência, que são aqueles previstos no art. 109 da Constituição de 1988.

[19] Só há exceção quando o crime é cometido contra ente público (art. 186, inciso III, do CP).

Aliás, o dispositivo em questão é desnecessário, uma vez que várias Polícias Civis contam com departamentos de combate a crimes cibernéticos[20] e devem investigar crimes de competência estadual. Além disso, o art. 1º, *caput*, da Lei 10.446/2002 já permite que a Polícia Federal empreenda investigações criminais quando os delitos tiverem repercussão interestadual ou internacional que exija repressão uniforme, o que é muito comum em crimes informáticos patrimoniais e em de violação de direitos de autor.

8. Dados cadastrais: silêncio do PLS 76/2000

Não se ocupou o projeto de definir "dados cadastrais", no que andou mal. Tais dados dizem respeito ao nome, endereço, telefone, email, qualificação pessoal, filiação e números de identificação de usuários de serviços de telecomunicação.

Aqui, o PLS 762/2000 está em descompasso com outros projetos destinados ao aperfeiçoamento da persecução criminal, a exemplo do PLS 209/2003, já aprovado no Senado e que trata da lei de lavagem de dinheiro. No seu art. 17-B, o PLS 209/2003 permitirá à autoridade policial e ao Ministério Público, independentemente de autorização judicial, o acesso aos dados *cadastrais* do investigado "*mantidos pela Justiça Eleitoral, pelas empresas telefônicas, pelas instituições financeiras, provedores de internet e administradoras de cartão de crédito*". No particular, na sua meta 25, a Enccla 2006 propôs a elaboração de um cadastro nacional de assinantes de telefonia fixa e móvel e de Internet, a cargo do Ministério das Comunicações e da Anatel, o que viria facilitar a identificação de autores e vítimas de cibercrimes.

Segundo o art. 18, n. 3, da Convenção de Budapeste o conceito de dados cadastrais não se confunde com o de dados de tráfego nem com os dados comunicados (conteúdo da sessão telemática), razão pela qual ditas informações cadastrais não estão sujeitas aos mesmos parâmetros de proteção (reserva de jurisdição).

9. A interceptação telemática no PLS 76/2000

O Poder Executivo enviou à Câmara dos Deputados o Projeto de Lei n. 3272/2008, que altera a disciplina da Lei 9.296/96, que regula a interceptação de comunicações telefônicas e telemáticas. O PLS 76/2000 era tímido neste tema e apenas buscava inserir um §2º ao art. 2º da Lei 9.296/96, para que fosse possível a interceptação telemática mesmo quando da investigação de crimes apenados com detenção.

[20] O art. 18 manda que os órgãos de polícia judiciária estruturem "setores e equipes de agentes especializados" no combate a cibercrimes.

Esta proposição não era harmônica com o PL 3272/2008 e foi suprimida na versão final do substitutivo aprovado no Senado em 2008. Segundo o art. 2º do PL 3278/2008, é possível a interceptação para a persecução de crimes apenados com reclusão e, "*na hipótese de crime apenado com detenção, quando a conduta delituosa tiver sido realizada por meio dessas modalidades de comunicação*". A proposição do Executivo é mais restritiva e, por ser a interceptação medida invasiva da vida privada, é mais adequada ao regime do art. 5º, X e XII, da CF, do que o que se pretendia no PLS 76/2000.

De qualquer modo, é essencial que a interceptação telemática também seja possível nos crimes apenados com detenção. Hoje só se admite a intervenção quando o fato investigado é crime sujeito a pena de reclusão (art. 2º, III, da Lei 9.296/96). Se aprovado o PLS 3272/2008, em qualquer crime informático (próprio ou impróprio), apenado com reclusão ou detenção, será possível a interceptação telemática, desde que cumprida a condição relacionada ao *modus operandi*.

10. Adequação do PLS 76/2000 à Convenção de Budapeste: um problema

Em novembro de 2001, ao final de um longo debate no seio do Conselho da Europa (CoE), adotou-se o texto final da primeira convenção internacional sobre cibercrimes, que se converteu no ETS 185[21] e entrou em vigor internacional em 1º de julho de 2004. Em maio de 2009, mais de duas dezenas de países haviam ratificado a Convenção de Budapeste, entre eles os Estados Unidos, a França, a Hungria, a Itália e a Alemanha.

A Convenção de Budapeste é o mais importante documento internacional de direito penal informático, servindo de norma-modelo para a regulamentação da cibercriminalidade em todo o mundo. Embora o tratado possibilite a adesão por nações não participantes do CoE, o Brasil ainda não manifestou interesse de tornar-se parte da Convenção, tampouco do Protocolo Adicional sobre Xenofobia e Racismo (ETS 189), tendo em vista a resistência do Ministério das Relações Exteriores[22].

A Convenção de Budapeste está dividida em três grandes eixos, contendo regras penais (tipificação de delitos informáticos), regras processuais e regras de cooperação internacional. Os dispositivos processuais estão nos arts. 14 a 22, englobando instrumentos úteis à persecução de crimes informáticos próprios e impróprios e para a obtenção de provas eletrônicas de um crime comum.

---

[21] *European Treaty Series.* Disponível em: http://conventions.coe.int/Default.asp. Acesso em: 17.maio.2009.

[22] Conforme manifestação da representante do MRE, Virgínia Bernardes de Souza Toniatti, por ocasião do Seminário Internacional sobre "Crimes Cibernéticos e Investigações Digitais", realizado pela Câmara dos Deputados, em Brasília, em 28 de maio de 2008.

Muitos dos temas regulados no tratado ficaram de fora do projeto do Senado, embora a exposição de motivos do substitutivo ao PLC 89/2003 (PLS 76/2000, no Senado) dê a entender que há plena harmonia com a Convenção de Budapeste. Não é o que se verifica, segundo entendemos. De fato, o substitutivo sequer se ocupa de estipular regras mínimas de cooperação penal internacional, algumas das quais são específicas para a persecução cibercriminal e que constam dos arts. 29 a 34 da Convenção. Além disso, como vimos, as disposições processuais do substitutivo são ainda criticáveis.

O certo é que, passados quase cinco anos da vigência internacional do ETS 185, é de se lamentar a inexistência de uma regulamentação abrangente da cibercriminalidade no Brasil, que compreenda regras bem postas de direito material e de direito processual. Apontamos[23] essa necessidade quando da apresentação do substitutivo do deputado Nelson Pellegrino ao PLC 84/1999. É preciso ter uma lei, mas não qualquer lei. Ainda há tempo de corrigir os equívocos do substitutivo do Senado e suprir suas omissões, a fim de que a ordem jurídica nacional faça frente à ameaça cibernética e possa harmonizar-se com a legislação de outros povos. Tal tarefa está agora entregue à Câmara dos Deputados. Cremos que o melhor caminho a seguir é, sem dúvida, aproveitar o paradigma da Convenção de Budapeste, que, se não vier a merecer a adesão do Brasil, ao menos poderá servir como lei-modelo para o País.

[23] ARAS, Vladimir. **Uma análise do substitutivo ao PL sobre crimes de informática.** Infoguerra, dez. 2002. Disponível em: http://www.infoguerra.com.br/infonews/talk/1039487091,39508,.shtml. Acesso em: 17.maio.2009.