ANPR
Associação Nacional dos Procuradores da República

# NOTA TÉCNICA PRESI/ANPR/ACA Nº 025/2011

**Proposição:** PL 84/1999

**Ementa:** Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), o Decreto-Lei nº 1.001, de 21 de outubro de 1969 (Código Penal Militar), a Lei nº 7.716, de 5 de janeiro de 1989, a Lei nº 8.069, de 13 de julho de 1990, e a Lei nº 10.446, de 8 de maio de 2002, para tipificar condutas realizadas mediante o uso de sistema eletrônico, digital ou similares, de rede de computadores, ou que sejam praticadas contra dispositivos de comunicação ou sistemas informatizados e similares, e dá outras providências.

**Autoria:** Deputador Luiz Piauhylino - PSDB/PE

**Relatoria:** Eduardo Azeredo – PSDB/MG

Senhor Deputado,

Trata-se de substitutivo do Senado Federal ao Projeto de Lei 84/1999, aprovado pelo Plenário da Câmara dos Deputados em novembro de 2003, que tipifica condutas operacionalizadas por meio da internet – os chamados crimes cibernéticos.

A Comissão de Segurança Pública, sob a relatoria do Deputado Nelson Pellegrino, apresentou parecer pela aprovação do substitutivo, mas ponderou que as alterações legislativas sobre os delitos informáticos devem ser feitas no Código Penal e não em lei extravagante, como na proposta original.

A referida Comissão sugeriu ainda a inserção de cinco novos tipos no Código Penal: o acesso indevido a meio eletrônico – hacking (154-A) –; a manipulação indevida de informação eletrônica (154-B); a difusão de vírus eletrônico (163-§3º); a divulgação de pornografia infantil (artigo 218-A); a falsificação de telefone celular ou meio de acesso a sistema eletrônico (298-A).

Por sua vez, a Comissão de Ciência e Tecnologia, Comunicação e Informática, sob a relatoria do Deputado Eduardo Azeredo, manifestou-se pela aprovação do projeto, da seguinte forma: supressão de todo o texto das expressões *"rede de computadores"* e *"dispositivos de comunicação"*; aprovação do artigo 16, exceto dos incisos I e III; rejeição do artigo 22-III e dos §§ 2º e 3º; rejeição do artigo 20 do substitutivo.

O PLS encontra-se atualmente em debate na Comissão de Ciência e Tecnologia, Comunicação e Informática (CCTCI), tendo sido aprovado requerimento da Deputada Luiza Erundina e outros para realização de Seminário sobre o tema cibercrimes.

## II – CONTEXTO ATUAL

O desenvolvimento das tecnologias de informação e, principalmente, com o advento da internet, novas questões jurídicas surgiram, demandando respostas céleres do Estado.

A internet não pode ser compreendida como um espaço de liberdade absoluta, alheio a qualquer tipo de regulamentação, uma vez que possibilita a prática de delitos à distância e de forma anônima, com um poder de lesividade, por vezes, mais expressivo que os crimes convencionais.

Os crimes virtuais e/ou cometidos por meio ou com auxílio de um computador têm demonstrado grande incremento, na prática e nas técnicas, como resultado imediato de um mundo globalizado e da evolução da comunicação entre os países.

É dizer: tem-se atualmente modalidades de crimes que dependem diretamente de um computador e outros, reputados tradicionais, que passam a ter seu modus operandi sofisticado pelo auxílio de computadores.

Esse novo feitio de criminalidade não encontra óbice nas fronteiras físicas e possui como aliado o anonimato e o conhecimento para criar estruturas sofisticadas e mecanismos de proteção das ações delituosas. Estes delitos caracterizam-se pelo incremento na velocidade de consumação do delito; por sua alta lesividade, dado o número expressivo e exponencial de vítimas; pela possibilidade de programação; bem como pela dificuldade probatória que apresentam.

É de convir, ainda, que vulnerabilidade técnica dos consumidores/usuários em distinguir as atividades online legítimas das fraudulentas é fator favorável à proliferação dos cibercrimes.

Vê-se, portanto, a necessidade de uma legislação penal e processual apta à proteção dos bens jurídicos da sociedade da informação, tendo em vista o elevado potencial de lesividade e o desvalor da criminalidade informática.

A ANPR, por meio desta nota técnica, propõe-se a analisar alguns pontos do substitutivo do Senado e a conformidade deste com a Constituição Federal, com o Código Penal e com o programa normativo da Convenção de Budapeste.

A Convenção de Budapeste, em vigor desde 2004, é o mais importante documento internacional de direito penal informático, servindo de norma modelo para a regulamentação da cibercriminalidade em todo o mundo. Apesar de o Brasil não ter aderido aos termos da Convenção é importante que a legislação sobre cibercrimes não se distancie dos conceitos ali estabelecidos.

De todo modo 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. É preciso ter uma lei que faça frente à ameaça cibernética e possa harmonizar-se com a legislação de outros povos.

## III – ALTERAÇÕES NO CÓDIGO PENAL

O substitutivo aprovado no Senado anda bem ao tipificar o estelionato informático (phishing) – abandonando o conceito

de furto eletrônico –, mantendo a estrutura do estelionato simples (artigo 171 – §2º – VII do Código Penal).

Contudo, a redação proposta para o artigo 171 do Código Penal, contém três equívocos. O primeiro está no referido inciso VII do §2º, pois não exige que o "*código malicioso*" seja executado para que o crime se consume. De acordo com o dispositivo basta 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 de 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 caraterizar outro crime, mas não o de estelionato.

O segundo problema. O artigo 171-A, sugerido na versão anterior do substitutivo, era silente sobre a aplicabilidade da causa especial de aumento de pena prevista na redação atual do §3º do

artigo 171, que pune mais severamente o crime de estelionato cometido contra entidade de direito público.

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 artigo 171 do Código Penal, com o que estará mantida a estrutura atual do crime de estelionato, com suas formas equiparadas e a necessária majorante.

O terceiro equívoco é, na verdade, uma omissão, mais grave do que as anteriores. É que, diferentemente dos demais incisos do artigo 171–§2º do Código Penal, o novo inciso VII (estelionato eletrônico) não deixa claro dois elementos indispensáveis a este delito: **a intenção de lucro e o ânimo de causar prejuízo a outrem**.

Tal omissão enseja um conflito entre os tipos descritos nos artigos 171–§2º–VII (estelionato eletrônico) e 163-A–§1º (inserção ou

difusão de código malicioso seguida de dano), uma vez que os dois possuem estrutura típico-normativa semelhante, mormente 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 em seu artigo 21:

> *"Em geral o estelionato, 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 seguinte meios: §1º Usando-se de falso nome ou falsa qualidade: §2º Usando-se de papel falso ou falsificado"*.

No direito comparado, é de se ver que o Código Penal português[1] desconhece o crime de furto eletrônico. O artigo 221-I do CP lusitano cuida do crime de burla informática (estelionato), punindo-se 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.

[1] 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.

Cézar 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"*[2].

**Vê-se, portanto, a necessidade de alterar a redação do artigo 171-VII-§2º do Código Penal, de modo que fique expresso que a difusão do malware tem como finalidade última a obtenção de vantagem ilícita em prejuízo alheio**[3]. Para isto, pode-se aproveitar a experiência espanhola ou lusitana, ou seguir o formato do artigo. 8º da Convenção de Budapeste, e aperfeiçoar a redação do tipo penal de estelionato eletrônico, adequando-o à realidade brasileira.

Com efeito, o artigo 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"*.**

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

[3] 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.

Em função do modelo da Convenção dos Cibercrimes, **propomos a seguinte redação para o inciso VII do §2º do artigo 171 do Código Penal:**

> *"Art. 171 (Omissis).*
> *§2º. Nas mesmas penas incorre quem:*
> *….*
> *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 (Omissis).*
> *§4º Se o agente usa nome falso ou dados pessoais de terceiros, ou abusa do anonimato a pena é aumentada de sexta parte".*

O artigo 285-A[4] tipifica a conduta de acesso não autorizado a rede de computadores, dispositivo de comunicação ou sistema informatizado – hacking. Tal tipo não objetiva a tutela da propriedade intelectual; pune-se o simples acesso a sistema informático pertencente a terceiro, desde que haja medidas de segurança ativas,

[4] 284 – A – Acessar, mediante violação de segurança, rede de computadores, dispositivo de comunicação ou sistema informatizado, protegidos por expressa restrição de acesso:
Pena – reclusão, de 1 (um) a 3 (três) anos, e multa.
Parágrafo único. Se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática do crime, a pena é aumentada de sexta parte.

destinadas a impedir o acesso ilegítimo ou não-autorizado, como senhas, criptografia, segurança biométrica e firewalls.

É dizer: o hacking consiste na prática utilizada para obter, de forma ilegal, o acesso a sistemas de computador e dados privados armazenados por pessoas físicas, jurídicas ou órgãos governamentais ou para danificar equipamentos, aplicativos e programas, sempre mediante a quebra de códigos de segurança.

**Tendo como norma base a Convenção de Budapeste parece adequado que o termo "*informatizado*" seja substituído por "*informático*",** passando o artigo 285-A a ter a seguinte redação: *"Acessar, mediante violação de segurança, rede de computadores, dispositivo de comunicação ou* ***sistema informático****, protegidos por expressa restrição de acesso".*

O crime descrito no artigo 285-A tem a pena de 1 (um) a 3 (três) anos de reclusão e multa, salvo na forma prevista no parágrafo único, hipótese em que a pena será aumentada de um sexto. É o que ocorre se o agente *"se vale de nome falso ou da utilização da identidade de terceiros".*

Nesse ponto, alteração redacional também torna o preceito mais direto e abrangente: *"Se o agente usa nome falso ou dados pessoais de terceiros, ou abusa do anonimato, a pena é aumentada de sexta parte"*. Ainda assim cumprirá à doutrina e à jurisprudência esclarecer o conceito de *"nome falso"* nas relações virtuais.

Apesar de tais dificuldades, o artigo 285-A do Código Penal estará em consonância com o artigo 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.

Na sequência tem-se o artigo 285-B a tipificar a conduta de *"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"*– aparentemente distinta da descrita no artigo 285-A.

Tal como o seu antecessor o artigo 285-B não se destina a proteção dos direitos autorais. Não há falar em punir o intercâmbio de informações na internet e nem tolher a criatividade ou o livre fluxo de ideias. A conduta típica será a de invadir determinado sistema informático e obter dados ou informações.

**Assim, a conduta descrita no artigo 285-B deveria ser uma forma qualificada do delito de acesso ilegítimo, previsto no 285-A.** Contudo, o legislador optou por criminalizar essa conduta em outro tipo, supostamente autônomo, e, pior, atribuiu-lhe pena idêntica a da forma básica de hacking, a despeito da ação descrita no artigo 285-B possuir maior reprovabilidade penal, uma vez que o agente não se satisfaz com o acesso indevido, ele também obtém dados ou informações disponíveis no sistema invadido, e, por essa razão, lesa de forma mais incisiva os interesses do legítimo detentor ou titular dos referidos dados.

Para além disso, a obtenção ou transmissão de dados exige o prévio acesso ilegítimo/desautorizado, tipificado no artigo 285-A, por meio da quebra de medidas de segurança que afastem a restrição de acesso.

**Mais: a Convenção de Budapeste especifica que o crime de acesso ilegítimo pode ter como elemento subjetivo do injusto a intenção de obter dados informáticos, o que é mais reprovável do que simplesmente o acesso indevido.**

**O artigo 285-B ainda apresenta incompatibilidade entre o crime do caput e a forma agravada do seu parágrafo único,** que trata do "*fornecimento*" a terceiros de dado ou informação obtida sem autorização.

O núcleo do caput é composto pelos verbos **obter** ou **transferir**, logo abrange o núcleo **fornecer**: o agente que transfere dado que obteve indevidamente estará necessariamente fornecendo-o a terceiro. **Desse modo, são previstas penas distintas para condutas, em sua essência, análogas.**

**Desse modo, sugerimos a seguinte reformulação do artigo 285-A e a, consequente, supressão do artigo 285-B:**

> *'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:*

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

***§1º. Se, mediante o acesso não autorizado, o agente obtêm, 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 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".***

Com isso, o artigo 285-C, que cuida da modalidade de ação penal (pública condicionada à representação), passa a ser um parágrafo do artigo 285-A, acrescentando-se entre os entes públicos o Distrito Federal, que ali não estava, e suprimindo-se a menção às agências – redundante –, pois a natureza 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 de P2P e a**

**redes wi-fi continua sendo fato atípico, quando não se verificar a prática de violação de direitos autorais (art. 184 do CP), ou violações de sigilo funcional ou divulgações de segredos.**

## IV - DADOS CADASTRAIS – ARTIGO 16 DO PL 84/1999

**O artigo 16 do projeto não trouxe a definição de "*dados cadastrais*", no que andou mal. Tais dados dizem respeito ao nome, endereço, telefone, e-mail, qualificação pessoal, filiação e números de identificação de usuários de serviços de telecomunicação.**

Nesse ponto, portanto, há descompasso com outros projetos destinados ao aperfeiçoamento da persecução criminal. Inclusive, a Enccla 2006, em sua meta 25, 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.

Conforme o artigo 18, n. 3, da Convenção de Budapeste **o conceito de dados cadastrais não se confunde com os 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).**

## V - ALTERAÇÃO NO ESTATUTO DA CRIANÇA E DO ADOLESCENTE (LEI 8.069/1990) - ARTIGO 20 DO PL 84/1999

O artigo 20 do substitutivo do Senado propõe a alteração do caput do artigo 241 do Estatuto da Criança e do Adolescente. À época a redação avançava por prever neste tipo de conduta múltipla a ação de "*divulgar*" pornografia infantil, bem como por tornar indiferente o meio utilizado para a prática criminosa, com a expressão "*por qualquer meio*".

Todavia, o Estatuto da Criança e do Adolescente já tipifica de forma eficaz as referidas ações, pois a Lei 11.829/2008 cuidou das lacunas existentes, inclusive de forma mais ampla, ao alterar a redação dos artigos 240 e 241 e inserir os artigos 241-A e 241-B.

Desse modo, a ANPR entende inoportuna a alteração proposta.

## VI - ALTERAÇÃO DA LEI DA REPRESSÃO UNIFORME (LEI 10.446/2002) – ARTIGO 21 DO PL 84/1999

O artigo 21 do substitutivo 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.**

Com efeito, não nos parece adequada essa previsão, pois 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 (art. 109 da Constituição).

Aliás o dispositivo em questão é desnecessário, uma vez que várias polícias civis contam com departamentos de combate a crime cibernéticos 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 violação de direitos de autor.

Por essa razão, a ANPR manifesta-se contrariamente a alteração da Lei 10.446/2002.

**VII - ARTIGO 22 DO PL 84/1999**

O artigo 22 do substitutivo impõe ao *"responsável pelo provimento de acesso a rede de computadores"* uma série de obrigações. Antes de examiná-las, é necessário apontar a **falha na redação do caput, que só se refere aos provedores de acesso, deixando de regular as obrigações legais dos provedores de conteúdo e de aplicações de Internet**, de modo que o objetivo da Lei dos Cibercrimes pode ser 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 artigo 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 a guarda por 5 anos. **Observe-se que alguns dos crimes objetos do substitutivo ou previstos noutros diplomas terão penas superiores a 4 anos de 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 art. 241 do ECA. **Em todas essas situações, a prescrição da pretensão punitiva em abstrato ocorrerá em 12 anos, pela regra do art. 109-III do Código Penal. 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 reação de entidades representativas de provedores contra tal dispositivo[5]. Movimento semelhante se viu durante os trabalhos preparatórios da Convenção de Budapeste, que prevê prazo de guarda mínimo de 90 dias, prorrogáveis (artigo 16, n.2, do ETS 185).

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

Na verdade, conforme o projeto, os provedores têm duas obrigações distintas, a manutenção dos dados de tráfego 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. 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 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

cibercriminalidade. **É preciso assegurar tempo suficiente para que, ao longo de uma investigação, seja possível obter dados necessários à identificação dos ciberdeliquentes. O projeto de lei do marco civil da Internet prevê guarda por apenas um ano. Neste ponto, o PL 84/99 é superior.**

Outros equívocos são ainda identificados no artigo 22: o primeiro diz respeito a adoção errônea, no inciso I, do conceito de tempo GMT (Greenwich Mean Time), que, por ter conotação geográfica, **foi substituído pela especificação UTC (*Universal Time, Coordinated*)**, que é uma medida derivada do Tempo Atômico Internacional.

O segundo resulta da não-utilização, também no inciso I, da definição de dados de tráfego instituída pelo próprio substitutivo no artigo 16-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 provedor deve preservar os dados de tráfego e fornecê-los quando solicitados.**

O terceiro equívoco ressalta da utilização das expressões *"objetivo de provimento de investigação pública formalizada"*[6] e *"fornecê-los exclusivamente à autoridade investigatória mediante prévia requisição judicial"*. **O artigo 22-I 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"*), tais como as propostas por pessoas físicas e jurídicas para a tutela da honra, da intimidade, da imagem e da vida privada (art. 5º–IV e V da Constituição).**

Por sua vez, quarto equívoco, constante do artigo 22-II –, levanta óbice à eficiência e à rapidez da persecução cibercriminal, uma vez que **exige *"requisição judicial"* para um simples pedido de preservação imediata 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.**

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

**O artigo 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.

É dizer: **não há 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. Esta solução foi acertadamente adotada pelo projeto de lei do marco civil da Internet, que, neste aspecto (guarda de logs e procedimento de preservação), é superior ao PL 84/99.

Além disso, **o artigo 22-II nada diz sobre o prazo de conservação dos dados após a ordem judicial.** À primeira vista, este prazo deveria ser equivalente ao do inciso I, que é de três anos. **Mas, se bem observado o problema, ver-ser-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 artigo 22-III 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 artigo 22-§2º prevê-se a aplicação de sanção pecuniária a provedores de acesso, mediante **procedimento de feição administrativa**, conduzido pela autoridade "*judicial*" nos casos em que desatendida ordem judicial. Contudo, esta não é a melhor solução, uma vez que inexiste qualquer dispositivo semelhante na legislação penal[7]. Além disso, haveria uma superposição de infrações, já 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.**

[7] 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.

É de 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.**

Com efeito, o artigo 22-§2º merece ser excluído. Além das críticas já mencionadas, há ressaltar que o projeto afronta os princípios da isonomia e da razoabilidade ao não dispor a mesma sanção para o caso de desatendimento direto do dever de guarda dos dados de tráfego e na hipótese de devassa dos dados referidos no artigo 22-II, em caso de quebra de "*confidencialidade e inviolabilidade*". Por falta de previsão expressa, a multa do §2º também não se aplicaria quando houver o descumprimento do dever de informar, previsto no inciso III (notícia-crime), nem, tampouco, nos casos de recusa a submeter-se a auditoria mencionada no §1º.

O artigo 22-III tem, ainda, merecido severa oposição de usuários, internautas e ONGs, sob a crença de que estimulará injustiças

na internet e transformará provedores em fiscais de seus clientes. O dispositivo exige do 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 a perpetração haja ocorrido no âmbito da rede de computadores sob sua responsabilidade"*.

Malgrado sua sofrível redação, o artigo 22-III 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 artigo 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 dependa de representação e a comunicação não exponha o cliente a procedimento criminal"*. O mesmo ocorre com o artigo. 245 da Lei 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 as práticas ilícitas de phising.**

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 rede 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 artigo 184- §§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 artigo 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 artigo 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.

**Assim, 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 previsto no artigo 10 da Lei 9.296/96 ou os delitos descritos nos artigos 153 e 154 do Código Penal.

**Apenas 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 notícia crime na forma do artigo 22-III do PL 84/2009.**

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 – "*crime sujeito a*

*acionamento penal público incondicionado, cuja perpetração haja ocorrido no âmbito da rede de computadores sob sua responsabilidade*". A redação, porém, pode ser aperfeiçoada: "*crimes de ação penal pública cometidos nos seus serviços*".

Frise-se que o dever de colaboração decorre do direito fundamental à segurança, previsto nos artigos 5º e 144 da Constituição. Afinal, segundo este último dispositivo a segurança pública é dever do Estado, direito e responsabilidade de todos.

## VIII - CONCLUSÕES

Em síntese, sugere-se as seguintes modificações:

a) quanto ao crime de estelionato informático (artigo 6º do PL 84/1999)

a.1) esclarecer no artigo 171-§2º-VII que é condição para a consumação do crime, que o código malicioso seja executado em sistema informático;

a.2) esclarecer na redação do artigo 171-§2º-VII do Código Penal as elementares de intenção de lucro e ânimo de causar prejuízo a outrem.

Propõe-se, portanto, como forma de atender as questões acima relacionadas o seguinte texto:

> *"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"*** ;

a.3) dispor sobre a aplicação da causa especial de aumento constante do atual artigo 171-§3º do Código Penal também em relação aos crimes cibernéticos, o que ensejará o reposicionamento do §3º constante do artigo 6º do substitutivo do Senado, para o §4º do artigo 171;

b) quanto ao crime de acesso não autorizado a sistema informatizado (artigo 2º do PL 84/99)

b.1) alterar a redação do artigo 285-A, substituindo a expressão "*informatizado*" por "*informático*", mais adequada à Convenção de Budapeste;

b.2) alterar a redação da qualificadora constante do artigo 285-A – parágrafo único, a fim de torná-la mais clara: "*Se o agente usa nome falso*

*ou dados pessoais de terceiros, ou abusa do anonimato, a pena é aumentada de sexta parte";*

b.3) alterar o artigo 285-B, para discipliná-lo como forma qualificada do artigo 285-A, uma vez que, em essência, o delito é o mesmo;

b.4) retirar a qualificadora do 285-B, pois a conduta de quem fornece dados a terceiros ou informação obtida sem autorização já está abrangida no caput deste artigo (no núcleo transferir).

b.5) alterar o artigo 285-C, para discipliná-lo em parágrafo do artigo 285-A, pois apenas disciplina a forma de processamento da ação penal desses delitos.

Propõe-se, portanto, como forma de atender as questões acima relacionadas o seguinte texto:

> *"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:*
>
> *Pena – reclusão, de 1 (um) a 3 (três) anos, e multa.*
> *§1º. Se, mediante o acesso não autorizado, o agente obtêm, 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 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"*;

c) definir, no artigo 16 do PL 84/1999 o que são "*dados cadastrais*".

d) quanto ao crime de divulgação de pornografia (artigo 20 do PL 84/99)

d.1) supressão da alteração sugerida para os artigos 240 e 241 do Estatuto da Criança e do Adolescente (Lei 8069/90), uma vez que a conduta já está adequadamente disciplinada na lei.

e) quanto à alteração redacional do artigo 1º da Lei de Repressão Uniforme (artigo 21 do PL 84/99)

e.1) supressão da alteração sugerida para o artigo 1º da Lei de Repressão Uniforme (Lei 10.446/02), dados o potencial prejuízo à investigação criminal.

f) alteração do artigo 22 do substitutivo do Senado para:

f.1) incluir as obrigações legais dos provedores de hospedagem;

f.2) estabelecer no artigo 22-I prazos maiores para guarda dos dados de conexão, em atenção aos prazos prescricionais de vários delitos (12 anos), utilizar a indicação do referencial UTC – Universal Time Coordinated – em vez do GMT – Greenwich Mean Time –, por ser aquele mais adequado; estabelecer que o provedor deve "*preservar os dados de tráfego e fornecê-los quando solicitados*", em vez de arrolá-los um a um, por conferir melhor técnica ao texto legal; bem como retirar as expressões *"objetivo de provimento de investigação pública formalizada"*[8] e *"fornecê-los exclusivamente à autoridade investigatória mediante prévia requisição judicial"*, uma vez que tais expressões excluem de seu rol o querelante e impedem o acesso aos dados de tráfego em causas cível não-públicas;

f.3) alterar o artigo 22-II, para estabelecer expressamente a possibilidade de se obter, independentemente de requisição judicial, a preservação imediata de dados de tráfego ou outras informações necessárias à investigação, bem como a possibilidade de o membro do Ministério Público ter acesso direto aos dados de tráfego e às informações cadastrais

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

de usuários de sistemas informáticos públicos, por estes não estarem resguardados pelo sigilo;

f.4) alterar o termo "*denúncia*" constante do artigo 22-III para "*notícia-crime*", por ser mais técnico;

f.5) retirar o artigo 22-§2º do projeto, uma vez que já existem mecanismos hábeis, inclusive, a previsão de crime, para os casos em que configurada desobediência a ordem judicial.

Tais as circunstâncias, a **ANPR**, propõe a adoção das alterações sugeridas, bem como a apreciação célere do projeto, dada a urgência de uma legislação penal sobre os delitos cibernéticos.

Brasília, 5 de setembro de 2011.



Vladimir Aras[9]
Diretor de Assuntos Jurídicos

[9] Vladimir Aras, é procurador da República na Bahia professor assistente de processo penal da Universidade Federal da Bahia (UFBA), mestre em Direito Público pela Universidade Federal de Pernambuco (UFPE) – ocasião em que analisou a Convenção sobre Cibercriminalidade do Conselho da Europa (Convenção de Budapeste), que disciplina a tipificação dos chamados crimes cibernéticos –, especializado em reforma processual penal latino-americana pelo Centro de Estudios de Justicia de las Americas (CEJA) e membro da International Association of Prosecutors.