Ordem dos Advogados do Brasil

Conselho Federal

Brasília - D.F.

Brasília, 20 de junho de 2007.

Exmo. Sr.
Senador Eduardo Azeredo
D.D. Relator do PLS 76
Em mãos

Ref.: Comentários sobre o texto do projeto de lei sobre de crimes de informática – PLS 76

Estimado Senador,

Atendendo a solicitação de V.Exa., apresentamos nesta oportunidade os comentários do Conselho Federal da Ordem dos Advogados do Brasil sobre o Projeto de Lei que tipifica os crimes de informática (PLS 76), na expectativa de que as sugestões ora encaminhadas possam ser encaminhadas a Comissão de Constituição de Justiça e de Tecnologia para maiores reflexões sobre o tema ora em trâmite no Senado Federal.

OBSERVAÇÃO GERAL

Concordamos integralmente com a crítica feita pela GV-Rio no sentido da "inadequação de estabelecer tipos penais em uma matéria que não foi legislada do ponto de vista civil, já que, sem o marco regulatório civil, é difícil à sociedade

avaliar quais são as condutas que devem ser proibidas pela legislação penal". Lança-se mão direto da sanção penal, a mais pesada do sistema, **regular** um setor do tráfego jurídico carente de regulamentação. É contraproducente que se procure regulamentar uma matéria diretamente através de proibições penais, cuja gravidade da sanção não deixa aos agentes ualquer margem de liberdade para a criação e retificação de conceitos.

Numa área cuja velocidade de transformação é tão alta quanto a área de informática (sistema/rede de dados/informações), é mais premente que o legislador se guie pelo marco da *ultima ratio*, utilizando a sanção penal tão-somente na ineficácia de outros meios punitivos.

Isto põe em evidência o acerto da critica da GV-Rio: se não temos sequer um marco regulatório extra-penal, utilizar do sistema penal como *prima ratio* da proteção é um erro que pode ter conseqüências gravíssimas para nosso País.

O projeto tem potencial altamente perigoso para o desenvolvimento informático em nosso País, devendo inspirar grande preocupação dos legisladores quanto à impermeabilidade que criará no nosso sistema quanto às evoluções tecnológicas vindas do estrangeiro. E, pior, em uma área cuja intersecção de sistemas nacionais e internacionais é essencial ao seu próprio funcionamento, com conseqüências possivelmente catastróficas para o exercício da atividade econômica e de educação, as que mais se utilizam tais sistemas.

Por outro lado, é preciso ter em vista observações já feitas por juristas de maior escol no sentido de que os "crimes de informática" não traduzem novos

bens jurídicos, mas, sim, são formas (meios) contemporâneas de se atingir bens jurídicos já existentes (pessoa, intimidade, patrimônio etc.). Por isso, parece-me inadequada a tutela pretensamente "autônoma" apresentada no Projeto. Talvez mais correto fosse, na tutela de cada bem jurídico já protegido no CP, criar-se uma nova modalidade de ataque (via sistemas de informática) com as penas conseqüentes.

Além disso, é importante salientar que apesar do "caput" do substitutivo preceituar que o seu teor visa apenas regulamentar os crimes de informática é importante ressaltar que o artigo 21 refere-se a norma de natureza cível, pois elenca uma série de obrigações as quais os provedores de acesso estarão sujeitas visando auxiliar durante o procedimento investigatório para determinar a identificação do que praticou ilícitos no meio eletrônico.

OBSERVAÇÕES PONTUAIS

ARTIGO 154-A

> **Acesso não autorizado a rede de computadores, dispositivo de comunicação ou sistema informatizado**
>
> Art. 154-A. Acessar rede de computadores, dispositivo de comunicação ou sistema informatizado, sem autorização do legítimo titular, quando exigida:
>
> Pena – reclusão, de 2 (dois) a 4 (quatro) anos, e multa.

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

Par 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.

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

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

Não sei se a colocação "geográfica" dos dispositivos (artigos 154-A, B e C) é das mais felizes, dentro dos crimes contra a pessoa. E, pior, a tutela dos demais bens jurídicos que podem vir a serem atingidos vem pulverizada no CP mediante as alterações propostas neste Projeto.

Pena de **reclusão de 2 a 4 anos** e multa: pena muitíssimo alta para um crime de perigo abstrato. O crime de invasão a domicílio, por exemplo, tem sanção de detenção de um a três meses! A violação de segredo profissional, detenção de 3 meses a 1 ano.

Os limites da sanção penal parecem ter sido "forçados" para cima em virtude do disposto no artigo 153, § 1º-A incluído no CP em 2000, que trata da divulgação de dados obtidos em sistema de informática e bancos de dados da Administração Pública (**pena de 1 a 4 anos de detenção**).

Observe-se, todavia, que a conduta acima referida tem um grau de antecipação da tutela menor, ou seja, implica em perigo maior ao bem jurídico tutelado, mesmo assim, a sanção revela-se mais branda na modalidade do que aquela que se quer cominar para conduta que implica em maior grau de antecipação da tutela.

Aquele que simplesmente "acessa rede de computadores" é punido mais severamente do que aquele que "divulga" dados obtidos em tal rede ou banco de dados.

A pena cominada a este tipo legal é, pois, um disparate e criará uma situação de inversão de valores no Código Penal.

Aliás, **há um desejo velado na lei de evitar a aplicação dos recursos da Lei n. 9.099/95**. Some-se a isto que chega a ser incongruente fazer a *persecutio* depender de representação e cominar pena de tamanha gravidade.

Parágrafo 4º (**defesa digital**): Concordo inteiramente com a observação crítica feita a este dispositivo, descriminalizando a "justiça feita com as próprias mãos" sem a previsão de uma situação concreta que torne a conduta legítima (art. 23 do CP). Se o caso é de exclusão da ilicitude por uma das situações previstas no artigo 23, então o dispositivo é desnecessário, mas, por sua amplitude exagerada, acaba ferindo as próprias bases do CP

ARTIGO 154-B

Obtenção, manutenção, transporte ou fornecimento não autorizado de informação eletrônica digital ou similar

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

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

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

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

Par 3º- 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.

Intolerável que conduta mais grave tenha pena menos severa do que a da conduta menos grave. A conduta prevista do artigo anterior está num grau de antecipação da tutela anterior, todavia é punida com maior severidade na modalidade de pena, que lá é de **reclusão**. Duas condutas que representam estágios diferentes de perigo ao bem jurídico tutelado não podem ser punidas de forma totalmente contraditória: a conduta mais grave com pena menos severa e a conduta mais grave com pena menos severa. Ainda que se alterasse a modalidade de pena (de reclusão para detenção no artigo anterior), continuaremos com um problema sério pela cominação idêntica a condutas de gravidade evidentemente diferentes. Violação ao princípio da proporcionalidade.

ARTIGO 153-C

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

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

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

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

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

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

V – código malicioso: o conjunto de instruções e tabelas de informações ou programa de computador ou qualquer outro sistema capaz de executar uma

seqüência de operações que resultem em ação de dano ou obtenção indevida de informações contra terceiro, de maneira dissimulada ou oculta, transparecendo tratar-se de ação de curso normal;

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

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

Afora as críticas técnicas feitas no documento enviado, chama a atenção o fato de que essas definições ficarão "geograficamente" mal localizadas no CP, isto

porque se aplicarão, necessariamente, a crimes que depois serão definidos em outro capítulo, "Do dano" e "Do estelionato e outras fraudes" (art. 163 e ss., CP).

ARTIGO 163-A

Difusão de Código Malicioso

Dano por Difusão de código malicioso eletrônico ou digital ou similar

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

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

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

Par 1º- Se o crime é cometido com finalidade de distribuição, inutilização, deterioração, alteração, dificultação do funcionamento, ou funcionamento desautorizado pelo titular, de dispositivo de

comunicação, de rede de computadores, ou de sistema informatizado:

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

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

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

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

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

Par 4º - Não há crime quando a ação do agente é a titulo de defesa digital, excetuado o desvio de finalidade ou o excesso.

• **Caput** ("criar, inserir ou difundir código malicioso"): Em primeiro lugar, a rubrica da figura ("Dano por difusão de código malicioso eletrônico ou digital ou similar") não expressa a verdadeira natureza do crime descrito que, ao contrário do nome, não é material, não exigindo a superveniência de dano para sua consumação. Na verdade, a rigor, não há punição de crime material doloso no projeto, só se pune o crime material culposo.

Punição de ato preparatório ("criar") que pode facilmente nunca desembocar em qualquer perigo para o bem jurídico tutelado. Violação do princípio da ofensividade. Pior, o ato preparatório é punido **com a mesma** pena de atos já executórios ("inserir" ou "difundir") e que implicam, ainda que em abstrato, perigo para o bem jurídico tutelado. Não conseguimos ver explicação racional para a modalidade de pena "reclusão".

Não bastasse, pode-se criar um código malicioso para ser usado no próprio sistema do titular para teste de segurança do próprio sistema. Pune-se, assim, uma conduta do tráfego normal dos sistemas de informação, que não visa lesar interesse jurídico alheio e que é orientada à própria tutela do bem jurídico.

§ 2º: A crítica que vem no texto é absolutamente pertinente. A punição da difusão culposa de código malicioso que causa dano em sistema alheio é o mais rematado absurdo porque, na verdade, incontrolável para a maior parte dos usuários de sistemas de informática. Aprovada tal norma penal, todos os usuários

de sistemas de informática, reiteramos **todos**, virão a um dia certamente cometer tal crime.

Além disso, é cediço que o crime culposo implica em menoscabo menor do bem jurídico do que o crime doloso, todavia, no projeto, a pena mais alta para as condutas previstas no artigo 163 é justamente a do crime culposo, que alcança o patamar de reclusão de 3 a 5 anos e multa, mais grave do que aquelas cominadas a quase todos os crimes dolosos contra o patrimônio (não pluriofensivos) e aos crimes econômicos *lato sensu* (crimes contra a ordem tributária, contra as relações de consumo, contra o sistema financeiro nacional, contra a ordem econômica etc.).

Artigo 171-A

Difusão de código malicioso

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

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

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

Par 2º - Não há crime quando a difusão ocorrer a título de defesa digital, excetuando o desvio de finalidade ou o excesso.

O tipo está muito mal redigido. A princípio parece um tipo de resultado cortado, mas no final da norma incriminadora há uma clara referência ao dano. Se houvesse mesmo dois tipos, já teríamos um problema com a cominação da sanção que seria idêntica para condutas de gravidade evidentemente diversa: um crime formal e um crime material. Além disso, este crime torna clara a inconsistência da sanção prevista no artigo 163-A que tem potencial lesivo nulo ou baixo, quando comparada a esta, e, todavia, recebe a mesma sanção.

Pior ainda quando comparada com a sanção cominada ao art. 154-A – reclusão de 2 a 4 anos e multa --, com pena de severidade muito maior para conduta que implica em perigo totalmente remoto para o bem jurídico tutelado.

Artigo 21.

Ao nosso ver o "caput" do artigo 21 não deve restringir apenas aos provedores de acesso as obrigações impostas por este artigo para a preservação e o fornecimento de dados mediante autorização judicial que serão necessárias para o processo investigatório da autoria dos ilícitos praticados pelo meio eletrônico.

Durante o processo investigatório de crimes contra honra praticados em sites de relacionamento é extremamente necessário para que se alcance êxito na identificação do autor que inseriu conteúdo ilícito na rede que haja a preservação do conteúdo capaz de identificar o agente com os dados armazenados pelos provedores de conteúdo.

Neste sentido, entendemos que a redação deveria ser genérica contemplando o seguinte "caput":
Art. 21 - "O responsável por liberar o acesso a uma rede de computadores ou prestar serviços mediante seu uso é obrigado a:"

É imperioso esclarecer que vários provedores de conteúdo que possuem sede no exterior e escritórios de representação no nosso país e que possuem serviços com grande audiência entre os brasileiros vêm hospedando conteúdo ilícito e vem descumprindo determinações legais do Judiciário Brasileiro no cumprimento de despachos que obrigam a sede nacional a prestar informações sobre a autoria do crime.
Além deste motivo, também em razão do principio da isonomia não há como admitir a existência de uma diferenciação de privilégios visando obrigar somente

os provedores de acesso em detrimento das demais categorias de provedores para preservar os dados das conexões realizadas em rede de computadores aptos a identificação do usuário.

Por estes motivos é imperioso que o caput do artigo 21 seja alterado para não restringir apenas aos provedores de acesso mas sim a todo responsável por liberar o acesso a uma rede de computadores ou aquele que prestar serviços mediante seu uso as obrigações impostas neste artigo.

Este é o nosso parecer.

S.M.J.

Brasilia, 20 de junho de 2007.

Alberto Zacarias Toron
Secretario Adjunto do Conselho Federal da OAB

Alexandre Atheniense
Presidente da Comissão de Tecnologia da Informação do Conselho Federal da OAB

Heloisa Estellita

Doutora em Direito Penal USP