3 críticas ao Projeto de Lei de Crimes Informáticos*

*Por **Túlio Vianna**, Professor de Direito Penal da PUC Minas*

Data da publicação:

Julho de 2009

Há 10 anos tramita no Congresso Nacional o projeto de lei nº 84/1999 que visa tipificar os crimes informáticos em nosso ordenamento jurídico. Aprovado na Câmara em novembro de 2003, o projeto foi enviado para apreciação no Senado onde tramitou sob o nº 89/2003 e recebeu substitutivos dos senadores Eduardo Azeredo e Aloizio Mercadante que acabaram culminando com a aprovação da sua redação final em 9 de julho de 2008. O projeto, então, retornou à Câmara dos Deputados, onde tramita atualmente.

Nossa proposta aqui é analisar os três artigos mais polêmicos do projeto e propor algumas soluções para seu aperfeiçoamento.

TÉCNICA LEGISLATIVA

Logo de início se percebe a péssima técnica legislativa do projeto que criou um novo capítulo no Código Penal completamente dissociado dos critérios que regem nosso código:

“CAPÍTULO IV DOS CRIMES CONTRA A SEGURANÇA DOS SISTEMAS INFORMATIZADOS”

É um consenso entre os penalistas brasileiros que os tipos penais são classificados de acordo com o bem jurídico protegido, ou seja, com o direito fundamental da pessoa humana que fundamenta a criminalização da conduta. Assim, temos crimes contra o direito à vida, contra o direito ao patrimônio, contra o direito à honra, contra o direito à liberdade sexual, etc.

Os direitos que se procuram resguardar com a criação destes crimes informáticos são o direito à propriedade dos dados informáticos (não se pode apagá-los ou modificá-los sem a permissão do dono) e o direito à privacidade destes dados (não se pode acessá-los sem a permissão do dono). Em um único conceito: inviolabilidade dos dados informáticos, entendida como a tutela simultânea da propriedade e da privacidade destes dados, tal como, na inviolabilidade de correspondência.

Destarte, os novos tipos deveriam constar nos arts.154-a e seguintes, logo após os crimes contra a inviolabilidade de correspondência (arts. 151 e 152) e inviolabilidade de segredos (arts. 153 e 154).

O legislador, porém, demonstrando sua pouca intimidade com regras básicas da dogmática penal, optou por posicionar os tipos logo após os crimes contra a saúde pública (art. 267-285).

SOLUÇÃO PROPOSTA

Criação da Seção V – Dos crimes contra a inviolabilidade dos dados informáticos no Capítulo VI, do Título I da Parte Especial do Código Penal, iniciando os novos tipos penais a partir do art. 154-a.

CRIMINALIZAÇÕES

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

Art. 285-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.*

O primeiro equívoco visível no art. 285-A é exigir que a conduta seja praticada com violação de segurança, o que implica na ausência de tipicidade da conduta do hacker que invade um computador doméstico não protegido por um firewall ou um antivírus. Seria o equivalente a permitir que um ladrão furte uma casa, tão-somente porque seu proprietário deixou a porta aberta. Um completo absurdo.

Não menos absurda é a necessidade de uma “expressa restrição de acesso”. O fato de alguém deixar seu notebook na mesa de um restaurante enquanto vai ao banheiro, não torna lícita a conduta de quem se aproveita desta ausência para acessar os dados. Não é razoável exigir que o proprietário tenha que declarar expressamente que ninguém está autorizado a acessar seus dados. Trata-se de uma restrição tácita elementar, não amparada, porém, pelo projeto Azeredo.

Por outro lado, a mesma lei que contém estas lacunas na proteção do usuário doméstico incauto, permite interpretações bastante rigorosas, já que a redação do tipo é bastante vaga.

Algum juiz poderia entender, por exemplo, que a restrição prevista neste artigo abarca a conduta de alguém que usa um crack (pequeno software para retirar restrições de acesso em softwares originais que visam a proteção de direitos autorais) para executar um jogo de computador sem a necessidade do uso do DVD.

Ainda que não pareça ser este o intuito do legislador, é preciso lembrar que, após aprovada uma lei, pouco importa qual era a pretensão original do legislativo, pois o juiz a interpretará de acordo com a sua livre convicção.Por fim, ainda em relação a este artigo, o parágrafo único prevê um aumento de pena para a hipótese de o agente se utilizar de nome falso para a prática do crime. Trata-se de mais um grave equívoco do legislador, que parte do pressuposto de que haverá casos em que o autor utilizará de seu nome verdadeiro para a prática do crime, o que é bastante improvável.

As qualificadoras só devem impor incremento de pena se – e somente se – a circunstância a ser utilizada como qualificadora demonstrar um plus de reprovabilidade da conduta do agente, isto é, uma gravidade maior daquela já punida pela pena do caput do artigo.

Em seguida, continua o projeto:

Obtenção, transferência ou fornecimento não autorizado de dado ou informação

Art. 285-B. 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:

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

Parágrafo único. *Se o dado ou informação obtida desautorizadamente é fornecida a terceiros, a pena é aumentada de um terço.*

Trata-se de uma conduta que é desdobramento natural da prevista no art. 285-A e, portanto, a boa técnica penal recomenda que seja abordada em parágrafos do artigo anterior e, não, de um novo tipo, pois, caso aprovado o projeto, o agente não poderia ser condenado simultaneamente nas iras do art. 285-a e 285-b, já que para obter ou transferir os dados (art. 285-b) é condição necessária que num primeiro momento ele os acesse (art. 285-a).

SOLUÇÃO PROPOSTA

Reescrever os arts. 285-a e 285-b, em um único artigo, dando-lhes uma redação mais objetiva e prevendo hipóteses privilegiadoras e qualificadoras que, de fato, demonstram uma menor ou uma maior reprovação social

da conduta. A título de sugestão:

Acesso não autorizado a sistemas computacionais

Art. 154-A. Acessar, sem autorização, dados ou programas em sistema computacional alheio.

Pena - detenção, de um a seis meses, ou multa.

§ 1º. A pena será reduzida de um a dois terços ou o juiz aplicará somente a pena de multa se o agente não inha intenção de lucro ou de obter vantagem de qualquer espécie para si ou para outrem e foi pequeno o prejuízo para a vítima.

§ 2º. Aumenta-se a pena de um terço até metade:

I. se o crime é cometido contra sistema computacional da União, Estado, Distrito Federal, Município, órgão ou entidade da administração direta ou indireta ou de empresa concessionária de serviços públicos;

II. se o crime é cometido por funcionário público ou por quem exerça a função de administrador de sistemas ou assemelhada, com abuso de poder ou com violação de dever inerente a função;

III. se o agente destrói ou danifca o sistema computacional ou os dados nele armazenados;

IV. se o agente divulga a terceiros as informações obtidas, causando dano material ou moral à vítima.

§ 3º. Somente se procede mediante representação, salvo na hipótese do § 2º, II, em que a ação é pública incondicionada.

Finalmente, cabe analisar o artigo mais polêmico do projeto:

VIGILÂNCIA

Art. 22. O responsável pelo provimento de acesso a rede de computadores mundial, comercial ou do setor público é obrigado a:

I. manter em ambiente controlado e de segurança, pelo prazo de 3 (três) anos, com o objetivo de provimento de investigação pública formalizada, os dados de endereçamento eletrônico da origem, hora, data e a referência GMT da conexão efetuada por meio de rede de computadores e fornecê-los exclusivamente à autoridade investigatória mediante prévia requisição judicial;

II. preservar imediatamente, após requisição judicial, outras informações requisitadas em curso de investigação, respondendo civil e penalmente pela sua absoluta confidencialidade e inviolabilidade;

III. informar, 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.

A ideia de que todo usuário de Internet tenha seus registros de acesso armazenados nos servidores por 3 anos é exageradamente invasiva e fere visivelmente o art.5º, **X**, da Constituição da República que dispõe:

X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;

Além do mais, se aprovado, o dispositivo inviabilizaria a inclusão digital por meio de redes sem fio (Wi-fi) em áreas de difícil acesso, tais como florestas, regiões interioranas com pouca infra-estrutura ou mesmo favelas, criando uma desnecessária e cara burocratização ao se exigir o cadastro prévio dos usuários.

Não bastasse a violação de privacidade dos usuários e a burocratização da redes de Internet sem fio, a proposta mostra-se bastante ingênua, pois criminosos e pessoas mal-intencionadas de uma forma geral, poderiam conseguir acesso à Internet com relativa facilidade em lan houses, com o uso de documentos falsos ou de

terceiros. Também não faltam recursos técnicos que permitam a usuários de computadores camuflarem seus endereços I.P., de modo que, mesmo que acessem de sua casa ou local de trabalho, seus atos não deixem rastros na rede.

Finalmente, o parágrafo terceiro cria ainda a obrigação de delação por parte do provedor de acesso, colocando os responsáveis pelo serviço na difícil condição de vigias dos atos de centenas ou milhares de usuários. Algo como exigir que as operadoras de telefonia delatem seus usuários quando houver indícios da prática de crimes em seus telefonemas. Dispositivo fadado a ser letra morta, portanto.

Em suma, o artigo imporia uma vigilância constante aos acessos do cidadão comum, dificultaria em muito a inclusão digital por meio de redes sem fio e, por outro lado, seria ineficaz no combate aos verdadeiros criminosos da Internet.

SOLUÇÃO PROPOSTA

A supressão integral deste artigo do projeto de lei.

À GUISA DE CONCLUSÃO

Finalmente, é preciso advertir o leitor de que o projeto é composto ao todo por 23 artigos e que só tratamos aqui de 3 deles, pois os consideramos eivados dos maiores equívocos.

Nosso silêncio quanto aos demais não deve ser interpretado, porém, como aprovação do texto, mas tão-somente, como uma estratégia para que não se perca o foco da discussão dos temas mais relevantes.

O conjunto do texto do projeto é muito fraco do ponto de vista técnico-penal e sua adequada reestruturação implicaria praticamente na criação de um novo projeto, razão pela qual, o melhor a se fazer atualmente é arquivar o presente projeto e criar uma comissão formada por professores de Direito Penal, professores de Ciência da Computação e representantes da sociedade civil para que construam democraticamente um novo texto que contemple os interesses dos brasileiros de uma Internet razoavelmente segura, preservando os direitos fundamentais da pessoa humana.

**A pedido do autor, este artigo não foi revisado e editado pela equipe da poliTICs – está publicado exatamente conforme o texto original por ele enviado.*

Categoria:

- poliTICs 4