São Paulo, 15 de agosto de 2008

Ao
Excelentíssimo Sr. Ministro de Estado da Justiça, Sr. Tarso Genro
Ministério da Justiça
Esplanada dos Ministérios, Bloco T, Edifício sede
70064-900 Brasília-DF

Assunto: Substitutivo do Senado ao Projeto de Lei da Câmara nº 89 de 2003

Excelentíssimo Sr. Ministro do Estado da Justiça, Sr. Tarso Genro,

O GPOPAI – Grupo de Pesquisa em Políticas Públicas para o Acesso à Informação da Escola de Artes, Ciências e Humanidades da Universidade de São Paulo vem por meio desta apresentar a sua contribuição com relação ao Substitutivo do Senado ao Projeto de Lei da Câmara nº 89 de 2003, de autoria do Senador Eduardo Azeredo, que pretende tipificar certas condutas realizadas no âmbito da rede mundial de computadores ou mediante o uso de tecnologias digitais, eletrônicas ou similares.

1. A matéria tratada pelo Projeto é de grande relevância. A Internet e as tecnologias digitais, eletrônicas e similares trouxeram uma série de benefícios e potencialidades (como redução dos custos de comunicação e de produção da cultura, ampliação do acesso e democratização da produção cultural, entre outras) e revolucionaram a forma como hoje se comunica e se produz a cultura.

2. O Projeto ora analisado parece-nos caminhar na contramão dessas tendências. Ao invés de fomentar a utilização aberta e democrática das tecnologias digitais e eletrônicas, privilegiando o interesse público, ele atende apenas a interesses de instituições financeiras pressionadas pelos prejuízos gerados pelas fraudes bancárias na Internet, e da indústria do entretenimento norte americana, que pressiona pela adoção dos mecanismos tecnológicos de restrição de acesso e pela criminalização da quebra desses mecanismos[1]. Sob a justificativa de facilitar a investigação e punição de uma série de condutas ilegais (em grande parte já tipificadas[2]), e em virtude de seu texto excessivamente amplo e impreciso, o Projeto acaba por criminalizar práticas comuns e legítimas na Internet e em dispositivos digitais restringindo significativamente os seguintes direitos fundamentais: liberdade de expressão, direito à privacidade, direito à informação, direito à cultura e direito à comunicação. Os artigos 2º, 4º, 5º, 6º e 22º do Projeto são os que apresentam maior potencial de dano.

3. O artigo 2º prevê a inclusão dos artigos 285-A e 285-B no Código Penal visando à criminalização do acesso "*mediante violação de segurança, rede de computadores, dispositivo de comunicação ou sistema informatizado, protegidos por expressa restrição de acesso*" e o ato 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*".

Além de contar com definições imprecisas como "titular da rede de computadores" ou "titular do dispositivo de comunicação" (consumidor proprietário do equipamento ou empresa que o criou com a proteção?), a conduta descrita por esses artigos vai muito além da proibição da violação de sistemas bancários. O termo "restrição de acesso" não é definido no Projeto e pode indicar uma restrição legal, contratual ou tecnológica. Tais restrições podem (i) impedir o exercício de direitos legítimos dos usuários, permitidos pela Lei do Direito Autoral, como o desbloqueio de um DVD que contenha uma obra não protegida por direito autoral e (ii) obstar a fruição de direitos básicos do consumidor, como a garantia de interoperabilidade entre os equipamentos. Vale dizer também que a a pena proposta para tais condutas é excessiva e desproporcional se comparada com outros crimes previstos no Código Penal. Os artigos criados

pelo Projeto prevêem pena de reclusão de 1 a 3 anos e multa, equivalendo-se, por exemplo, à pena de crimes como o homicídio culposo e seqüestro e cárcere privado, e superando a pena pelo crime de maus-tratos (2 meses a um ano) ou abandono de recém nascido (detenção de 6 meses a 2 anos). Desbloquear um celular ou transferir músicas de um computador para um tocador de um mp3 torna-se mais grave que abandonar uma criança. Observamos, ademais, que a criminalização destas práticas com penas excessivas é uma demanda da indústria do entretenimento americana, manifesta no último relatório da associação americana da indústria do direito autoral[3].

Em suma, os mecanismos de restrição de acesso não podem ser protegidos com tutela penal pois restringem o exercício de direitos legítimos. A não existência desse tipo penal não impede, contudo, que práticas ilegítimas ou danosas sejam punidas, seja em virtude da violação de direitos do autor (crime tipificado no artigo 184 do Código Penal[4]) ou em virtude do crime de dano (previsto no Artigo 163 do Código Penal[5]).

4. O Artigo 5º tipifica a conduta de "*inserção ou difusão de código malicioso em dispositivo de comunicação, rede de computadores, ou sistema informatizado*", e estipula um aumento de pena caso a conduta resulte em "*destruição, inutilização, deterioração, alteração, dificultação do funcionamento, ou funcionamento desautorizado pelo legítimo titular, de dispositivo de comunicação, de rede de computadores, ou de sistema informatizado*", e o Artigo 6º criminaliza a difusão "*por qualquer meio, de código malicioso com intuito de facilitar ou permitir acesso indevido à rede de computadores, dispositivo de comunicação ou sistema informatizado*".

A conduta descrita penaliza o desenvolvimento de códigos que provoquem "*alteração no funcionamento de dispositivo de comunicação, de rede de computadores ou de sistema informatizado*", prática comum e necessária ao desenvolvimento da indústria de softwares. Não é requerido para a configuração do crime o dano, apenas a inserção ou difusão de código malicioso, o que caracteriza a punição de ato preparatório – o dano torna-se aí apenas uma causa de aumento de pena. A própria difusão do código malicioso através do computador de um usuário sem que ele saiba passa a estar sujeita a pena. Assim como no Artigo 2º as penas previstas também são excessivas (reclusão, de um a três anos, ou em caso de aumento de pena, reclusão, de dois a quatro anos, e multa), e a conduta efetivamente danosa (danos provocados por difusão de vírus) pode já ser punida por meio do Artigo 163 do Código Penal (crime de dano), sem que seja necessária a alteração desse Artigo, conforme proposto pelo Artigo 4º do Projeto.

5. O Artigo 22, que estabelece aos responsáveis pelo provimento de acesso à rede de computadores a obrigação de "*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*" entra em colisão com uma série de direitos fundamentais, quais sejam, a liberdade de expressão, direito à privacidade, direito à informação, direito à cultura e o direito à comunicação.

Primeiramente, é importante destacar que os dados a serem colhidos conforme o Artigo 22 não são meros dados identificadores não protegidos pelo Inciso XXII do Artigo 5º da Constituição Federal, como argumenta o parecer da Comissão de Constituição, Justiça e Cidadania da Câmara dos Deputados ("CCJ"), mas sim dados pessoais e particulares que envolvem relações de convivência privada e hábitos dos usuários da Internet. Os registros não informarão meros elementos identificadores como nome, identidade e filiação do usuário, que são dados que não se alteram com freqüência, mas sim o endereço, data e hora de todos os seus acessos à Internet que revelam não uma situação estável, mas um fluxo, uma relação entre o usuário e o serviço acessado, constituindo assim um verdadeiro relatório da utilização de um serviço público e dos hábitos de acesso à Internet desses usuários.

Utilizando a mesma jurisprudência[6] e a mesma doutrina citadas pela CCJ[7], somos levados a divergir dela e concluir que os dados a serem armazenados conforme o artigo 22 do Projeto não são meros dados identificadores e permanentes mas referem-se justamente à comunicação de dados privativos de cada sujeito, protegidos pelo Inciso XXII do Artigo 5º da Constituição Federal[8] – dados que se explorados por terceiros, podem colocar em risco a integridade moral do indivíduo. Não refutamos que esse direito à privacidade possa colidir com algum interesse público que justifique a restrição a essa tutela. Contudo, a realização dos registros deve ocorrer apenas em um momento posterior à colisão desse direito e de uma forma direcionada à conduta suspeita[9], e não de forma prévia e geral, atingindo todos os usuários e com armazenamento de dados por um período tão longo (3 anos) como pretende o Projeto.

Analisando a colisão entre os direitos fundamentais restringidos e a necessidade de dados para as investigações de condutas ilegais realizadas na Internet, somos levados a reconhecer a inconveniência e a ineficácia da regra proposta pelo Artigo 22. Isso porque:

(I) Esta regra não é um meio adequado e eficaz para atingir o fim que almeja (conferir às autoridades administrativas meio eficaz de buscar os autores dos crimes praticados pela Internet) pois ela pode ser facilmente contornada pelos verdadeiros criminosos da Internet. Estes poderão facilmente garantir seu anonimato através de servidores *proxy* sediados no exterior que podem redirecionar o acesso e mascarar a identidade – uma medida simples que não requer grandes conhecimentos técnicos e que torna as medidas adotadas no Artigo 22 inócuas; e

(II) A medida proposta também não é necessária pois não é o único meio nem o menos danoso de obter o fim almejado. Primeiramente, o prazo previsto de armazenamento das informações é excessivamente alto. A Convenção de Cibercrime, por exemplo, que apesar de não ter sido elaborada nem assinada pelo Brasil é colocada como inspiração desse Projeto, recomenda a proteção por um período máximo de 90 dias. Além disso, há outras opções menos amplas e mais dirigidas que causam menor prejuízo aos direitos fundamentais. Como exemplo, os registros poderiam ser autorizados e realizados apenas após autorização judicial, no curso das investigações, quando houver indícios de autoria do crime devidamente apontados. Isso evitaria a abrangência extremamente ampla proposta pelo Projeto que visa a guardar informações de todos os usuários de Internet do país.

A ameaça aos direitos fundamentais não é, portanto, aceitável, pois a extensão dos benefícios obtidos com esta regra (limitada, como vimos) não justifica a extensão da restrição imposta aos direitos fundamentais (ampla) que ela empreende. A medida obrigará a vigia de todos os usuários comuns da Internet e não será útil para a investigação dos verdadeiros criminosos, que tem meios simples de escapar à essa vigilância. Ademais, a geração de um banco de dados pessoais dessa magnitude não se mostra conveniente em um país com baixa tradição de respeito ao direito à privacidade. Exemplos disso são os mais de 400 mil grampos realizados no ano passado e a venda, por camelôs, de dados sigilosos da Receita Federal.

6. O Inciso III do Artigo 22, que obriga os provedores a "*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*", cria para o provedor uma obrigação a nosso ver indevida e desnecessária, dado a existência de órgãos administrativos competentes para a recepção de denúncias. Trata-se de uma obrigação que traz mais ônus do que vantagens, pois implica em gastos pelos provedores para cumprir uma função que originalmente pertence aos órgãos administrativos com poder de polícia.

7. As imperfeições do Projeto evidenciam o quanto é inadequado a aprovação de uma regulamentação penal antes da aprovação de um marco civil que estabeleça quais usos são os objetivos considerados legítimos para a Internet e para as tecnologias digitais, eletrônicas e similares.

Com base nessas considerações, sugerimos que sejam vetados ao menos os artigos 2º, 4º, 5º, 6º e 22º. Ao nosso ver, além de terem uma eficácia questionável, eles trazem graves prejuízos aos direitos fundamentais à privacidade, à informação, à comunicação, à cultura e à liberdade de expressão.

Renovando nossos protestos de consideração e apreço, subscrevemo-nos.

GPOPAI - Grupo de Pesquisa em Políticas Públicas para o Acesso à Informação da Escola de Artes, Ciências e Humanidades da Universidade de São Paulo:

Professora Dra. Gisele S. Craveiro, professora do curso de Sistemas de Informação da Universidade de São Paulo.

Professor Dr. Jorge A. S. Machado, professor do curso de Gestão de Políticas Públicas da Universidade de São Paulo.

Professor Dr. Pablo Ortellado, professor do curso de Gestão de Políticas Públicas da Universidade de São Paulo.

Alcimar Silva de Queiroz, mestre e doutorando em sociologia da educação pela Universidade de São Paulo.

José Paulo Guedes Pinto, mestre em economia pela Universidade Federal do Rio Grande do Sul e doutorando em economia pela Universidade de São Paulo.

Bráulio Santos Rabelo de Araújo, bacharel em direito e mestrando em direito econômico pela Universidade de São Paulo.

Eduardo B. Barbosa, sociólogo formado pela Universidade de São Paulo.

Cristiana Gonzalez, graduanda em Relações Internacionais pela Universidade de São Paulo.

Jamila Venturini, graduanda em jornalismo pela Universidade de São Paulo.

Luis E. T. Leon, graduando em Gestão de Políticas Públicas pela Universidade de São Paulo.

Rodolfo L. Castanheira, graduando em Ciência da Computação pela Universidade de São Paulo.

Rodrigo B. de Almeida, graduando em Sistemas de Informação pela Universidade de São Paulo.

Sarah Elizabeth Floriano Machado, graduanda em Gestão Ambiental pela Universidade de São Paulo.

Thais Carrança, graduanda em comunicação social pela Universidade de São Paulo.

1 "*Controle sobre a Produção de Mídia Ótica: Nos últimos anos, alguns países como Brasil, Indonésia, Malásia, Nigéria, Paquistão, Filipinas e Ucrânia progrediram no sentido de implementar controles na produção de mídia ótica. (...)* ***Os Estados Unidos continua a pressionar seus parceiros comerciais que enfrentam pirataria de mídia ótica em seus territórios para aprovarem legislação mais efetiva e aplicar agressivamente as leis e regulações existentes***" Secretaria de Comércio dos Estados Unidos (Office of The United States Trade Representative), In: **2008 Special 301 Report**.

2 A fraude bancária praticada pela Internet, utilização de códigos maliciosos para, por exemplo, roubo de senhas (pishing) são condutas geralmente enquadradas nos tipos de furto qualificado por fraude (Artigo 155, Parágrafo 4o, Inciso 2 do Código Penal) ou estelionato (Artigo 171 do Código Penal), não havendo, portanto, qualquer impedimento para a investigação e a punição desses crimes. Conforme Jurisprudência: HABEAS CORPUS nº 200401000494035, TRF, Primeira Região, Terceira Turma, Maranhão. ESTELIONATO. **CRIME PRATICADO PELA INTERNET**. PRISÃO PREVENTIVA. INEXISTÊNCIA DOS REQUISITOS. 1. **Crime de estelionato praticado pela internet**, com a participação, segundo o que consta do inquérito, de diversas pessoas, com atuações determinadas – a) **o programador (o que cria a página clone, os programas, ex. o Trojan ou cavalo de Tróia) - responsável pela captura da senha; é o cracker, não hacker**, b) o usuário (o explorador direto do programa), ou seja, o operador do programa; c) o plaqueiro, (de placa), biscoiteiro ou cartãozeiro (responsável pela aquisição dos cartões bancários e pela arrecadação de boletos que serão pagos via internet); d) sub-plaqueiro (a pessoa que, apesar de não conhecer os usuários do programa, compra os cartões magnéticos dos laranjas e os vende a plaqueiros que mantém contato com o usuário; **e) o laranja (o que empresta sua conta para receber os créditos espúrios da internet) - com a finalidade de pescar (obter mediante ardil) a senha de correntistas [pishing = password (senha) + fishing (pescaria)] e retirar dinheiro de suas contas bancárias**. (...) [grifo nosso]

3 "*Penas não dissuasivas: A APCM (Associação Anti-pirataria de Cinema e Musica) relata que as condenações cresceram mais de 500% (criminais), sendo 152 condenações por pirataria audiovisual e musical. A maior parte das condenações ocorreram nos Estados de São Paulo e Rio. Para colocar esse número em seu próprio contexto, vale notar que mais de 80% das condenações resultaram na sentença mínima de 2 anos, e que essas sentenças são normalmente suspendidas, e os piratas raramente ou nunca passam tempo na prisão. A legislação brasileira permite a suspensão de sentenças para réus primários, e a definição de réus primários é tão ampla que apenas acusados condenados por sentença irrecorrível são réus reincidentes.* ***Em outras palavras, o sistema brasileiro permanece longe de atingir o nível necessário de sentenças dissuasivas que contribuiriam para diminuir significativamente o nível de pirataria no mercado e desencorajar os criminosos de se engajarem nesses empreendimentos criminosos e lucrativos.***" International Intellectual Property Alliance Brazil, In: **2008 Special 301 Report**. . No ano anterior, o relatório recomendou explicitamente mudanças no "*código penal para aumentar as penalidades para a pirataria de forma a remover sanções menores e alternativas, tais como o serviço comunitário.*" International Intellectual Property Alliance Brazil, In: **2007 Special 301 Report**.

4 Artigo 184 do Código Penal: Violar direitos de autor e os que lhe são conexos: Pena – detenção, de 3 (três) meses a 1 (um) ano, ou multa.

5 Artigo 163 do Código Penal: Destruir, inutilizar ou deteriorar coisa alheia: Pena – detenção, de 1 (um) a 6 (seis) meses, ou multa.

6 "*Não entendo que se cuide de garantia com status constitucional. Não se trata da "intimidade" protegida no Inciso X do Artigo 5º da Constituição Federal. Da minha leitura no Inciso XII da Lei Fundamental, o que se protege, e de modo absoluto, até em relação ao Poder judiciário, é a comunicação "de dados" e não os "dados", o que tornaria impossível qualquer investigação administrativa, fosse qual fosse*" (voto proferido no MS n. 21.729-4/DF, DJ 19.10.2001) [grifos nossos].

7 "*Pelo sentido inexoravelmente comunicacional da convivência, a vida privada compõe, porém, um conjunto de situações que, usualmente, são informadas sem constrangimento. São dados que, embora privativos, como o nome, endereço, profissão, idade, estado civil, filiação, número de registro público oficial, etc, condicionam o próprio intercâmbio humano em sociedade, pois constituem elementos de identificação que tornam a comunicação possível, corrente e segura. Por isso, a proteção desses dados em si, pelo sigilo, não faz sentido.* ***Assim, a inviolabilidade de dados referentes à vida privada só tem pertinência para aqueles associados aos elementos identificadores usados nas relações de convivência as quais só dizem respeito aos que convivem. Dito de outro modo, os elementos de identificação só são protegidos quando compõem relações de convivência privativas: a proteção é para elas e não para eles. Em conseqüência, simples cadastros de elementos identificadores (nome, endereço, R.G., filiação, etc) não são protegidos. Mas cadastros que envolvam relações de convivência privada*** *(por exemplo, nas relações de clientela, desde quando é cliente, se a relação foi interrompida, as razões pelas quais isto ocorreu, quais os interesses particulares do cliente, sua capacidade de satisfazer aqueles interesses, etc) estão sob proteção.* ***Afinal, o risco à integridade moral do sujeito, objeto do direito à privacidade, não está no nome, mas na exploração do nome, não está nos elementos de identificação que condicionam as relações privadas, mas na apropriação dessas relações por terceiros a quem elas não dizem respeito***". In Tércio Sampaio Feraz Júnior, *Sigilo de Dados: O Direito à Privacidade e os Limites à Função Fiscalizadora do Estado*, Revista da Faculdade de Direito USP, vol. 88, 1993, p. 449. [grifos nossos]

8 Artigo 5º, XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal.

9 "*Destarte, embora o direito que assegura à inviolabilidade e à privacidade – art. 5º, X e XII, da CF – não seja absoluto, devendo ceder diante do interesse público superior, é necessário, contudo, que a implementação da medida que resulte na invasão de tais garantias constitucionais, seja precedida pela existência de indícios que apontem, de forma consistente, para a efetiva ocorrência de prática delituosa, e que não exista outro caminho para o aprofundamento da investigação, sob pena de restar frustrado todo o trabalho dirigido ao esclarecimento dos fatos;(...)*" Acordão do Tribunal Regional da Segunda Região, Rio de Janeiro, Habeas Corpus 3031, 200302010035354.