Artigo publicado no Jornal Valor Econômico do dia 27/07/2011

CYBERCRIME

Fernando Neto Botelho **(*)**

A Câmara dos Deputados se vê diante de um dilema. Projeto de lei de sua própria iniciativa – o famoso PL 84/99 (Lei de cybercrimes) – arrisca transformar-se em ácido desafio ao poder de auto-definição da Casa.

Iniciado em 1999, voltado para a repressão dos crimes eletrônicos, o projeto tramita, há 12 anos, no Parlamento. Aprovado pela própria Casa que o iniciou, foi ao Senado, onde recebeu texto substitutivo de sua versão original. Aprovado por unanimidade em julho/2008 pelo voto de Senadores da oposição e da situação, retornou, então, à Casa de origem, para votação conclusiva da superposição de textos (da própria Câmara e do Senado).

O problema surge aí. Primeiro, porque, ao receber, de volta, projeto modificado pelo Senado, a Câmara, regimentalmente, não pode imprimir-lhe modificações essenciais. Pode suprimir disposições, expressões, criadas pelo Senado, desde que não altere a essência votada. No máximo, pode rejeitar alterações da Casa Alta. Mas, se o fizer – se rejeitá-las – fará prevalecer seu próprio texto (no caso, o iniciado e aprovado, por Ela, a partir de 1999).

Parece um xadrez. A rigor, é o mecanismo regimental de solução do conflito de vontades legislativas de uma Casa parlamentar e Outra, que a Constituição assegura.

Mas, o aspecto dificultador desta atuação definidora da Câmara, quanto aos cybercrimes, surge de um ponto conseqüente a estas possibilidades.

Está ligado ao tema do projeto. A Câmara, se recusar a vontade unânime do Senado, terá que entregar à sanção presidencial sua própria visão, expressa no texto por Ela votado há anos. Dará à sociedade a informação de que os 12 anos de tramitação dos crimes eletrônicos no Brasil serviram para acentuar que os Senadores não terão tido a melhor visão do cybercrime brasileiro e que esta deve ser a mais antiga; não, a mais nova do Parlamento.

Democracia representativa funciona assim. Há que se respeita-la. Se a visão da Câmara que iniciou o projeto for esta, que se conclua a votação, que, neste momento, completa seu último biênio de indefinição, desde o momento em que retornado o projeto à Casa de origem. O projeto retornou às Comissões de Ciência e Tecnologia, Constituição e Justiça, e de Crimes Financeiros, que realizaram, neste último semestre, duas novas audiências públicas para análise do texto do Senado.

O fato é que, abertas as apostas sobre a prevalência do texto final – se o antigo, da Câmara; se o novo, do Senado – uma comunidade ampla aguarda o desfecho.

Nela, estão em jogo interesses corporativos, públicos e privados, e individuais; interesses que, para ficar no campo dos serviços públicos do Estado, assustou-se, por exemplo, com a ousadia de recentes ataques cibernéticos, de alta tecnologia, a sites do governo federal (20 páginas atacadas) e municipal (mais de 200 sites atacados, muitos retirados do ar, por crackers e pichadores eletrônicos); ataques que, pela sofisticação do meio usado (*botnets* criaram centenas de computadores zumbis, dentro e fora do país, com instalação oculta de vírus e códigos maliciosos, que tornaram computadores de usuários ferramental de serventia à distância, por *nerds* ultra-especializados), só puderam ser percebidos quando já haviam sido subjugados e ridicularizados por mensagens de protesto os sites públicos.

Essa engenharia do mal, que monopoliza o conhecimento (da computação sofisticada e dos protocolos de rêdes), cresce à sombra da impunidade gerada por insuficiência regulamentar de desatualizados instrumentos legais do país, como o Código Penal de 1.940.

Para cuidar da nova realidade, só lei atualizada. A tecnologia, sozinha, não dará conta. Só a lei garante oportunidade de defesa e prova justa, próprias das Democracias amadurecidas.

O Brasil se integrará a cenários internacionais se a tiver. Nesses cenários, aliás, por adesão histórica a antiga Convenção (Européia, de cybercrimes), quase 50 países não só da Europa, mas da Ásia, África, Américas do Norte e do Sul, já se adiantaram, instrumentalizando-se com leis de combate ao cyberterroristmo.

O projeto de lei sob definição da Câmara cumpre o papel de atualizar o Código Penal brasileiro/1940, dando-lhe 11 novos crimes eletrônicos, de alta tecnologia, como o ataque cibernético, a pixação eletrônica, a difusão de vírus, a pescaria e o estelionato com uso de rêdes.

50 milhões de internautas/Brasil (setembro/2010 – Ibope/Nielsen) têm direito a esta adequação. O 5º país/mundo em número de conexões/web, o 1º no ranking mundial do tempo médio de navegação/internet, o detentor do "record" de vendas em 2.010 pela internet, o possuidor de 60 milhões de computadores (previsão de 100 milhões para 2.012), o prestador inédito de serviços públicos eletrônicos, o promotor do sistema financeiro de pagamentos (ebanking no Brasil internet-banking adotado por 14% da população), o implementador de 200 milhões de telefones celulares com 10% de smart-phones/internet móvel, não pode perder o bonde desta história.

O Brasil está compelido a disciplinar, agora, a ação de seus cybercriminosos.

---

* *Desembargador do Tribunal de Justiça/MG, da 8a. Câmara Cível. MBA em Gestão de Telecomunicações, pela Ohio University/FGV-USA. Autor do livro "As Telecomunicações e o FUST" e Co-autor dos Livros "Direito Tributário das Telecomunicações" e "Direito das Telecomunicações e Tributação". Membro da ABDI - Associação Brasileira de Direito de Informática e Telecomunicações. Ex-Presidente da Comissão de TI-Tribunal de Justiça de Minas Gerais. Ex-Membro do CGTI do Conselho Nacional de Justiça. Ex-Coordenador da Comissão do Processo Eletrônico do TRE-MG. Professor da EJEF-Escola Judicial Desembargador Edésio Fernandes da Cadeira Direito Eletrônico, Tributação, e Crimes Eletrônicos dos Cursos. Autor de artigos, palestras, e trabalhos doutrinários sobre regulação e tributação de telecomunicações e TIC.*