Normas para punir o cibercrime no Brasil tornam-se um desafio

Artigo originalmente publicado na edição desta quarta-feira (27/7) do jornal Valor Econômico

A Câmara dos Deputados se vê diante de um dilema. Projeto de lei de sua própria iniciativa – o famoso PL 84, de 1999 (Lei de Cibercrimes) – arrisca transformar-se em ácido desafio ao poder de autodefinição 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 de 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 e expressões criadas pelo Senado, desde que não altere a essência votada. No máximo, pode rejeitar alterações da Casa Alta. Mas, se o fizer, fará prevalecer seu próprio texto (no caso, aquele 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 cibercrimes surge de um ponto consequente a estas possibilidades. Está ligado ao tema do projeto. A Câmara, se recusar à 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 cibercrime brasileiro e que esta deve ser a mais antiga; não, a mais nova do Parlamento. Essa engenharia do mal cresce à sombra da impunidade por falta de lei atual.

Democracia representativa funciona assim. Há que respeitá-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, 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 redes), cresce à sombra da impunidade gerada por insuficiência regulamentar de desatualizados instrumentos legais do país, como o Código Penal de 1940. 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 à antiga Convenção (Europeia, de cibercrimes), 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 ciberterrorismo. 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 redes.

Cinquenta milhões de internautas no Brasil (setembro/2010 – Ibope/Nielsen) têm direito a essa adequação. O 5º país do mundo em número de conexões/web, o 1º no ranking mundial do tempo médio de navegação na internet, o detentor do "record" de vendas em 2010 pela internet, o possuidor de 60 milhões de computadores (previsão de 100 milhões para 2012), o prestador inédito de serviços públicos eletrônicos, o promotor do sistema financeiro de pagamentos (e-banking adotado por 14% da população), o implementador de 200 milhões de telefones celulares com 10% de smartphones com internet móvel, não pode perder o bonde desta história.

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