Rafael Maciel: Leis não tornarão meio digital mais seguro

O Senado Federal aprovou em plenário, no último dia 31, o Projeto de Lei originário da Câmara de Deputados (PL 2793/2011 e PLC 35/2012) que tipifica como criminosas algumas condutas cometidas no meio digital, sobretudo a invasão de computadores. A imprensa tem noticiado como se fosse a primeira aprovação desse tipo no Brasil e alguns setores comemoraram como se a existência de uma lei para os crimes eletrônicos fosse tudo o que faltava para diminuir a delinquência cibernética. Não se tem dúvida da importância do fato, entretanto, esse projeto ainda será encaminhado para a Câmara dos Deputados e lá poderá sofrer tal qual o PL 84/1999 encaminhado pelo Senado em 2008 e até o início deste ano aguardava votação.

Pelo menos agora, nos parece, será conduzido com maior celeridade, sobretudo por ter o PL 84/1999 sido praticamente extinto, porquanto excluídas as condutas lá previstas em um acordo celebrado com o governo federal no calor do caso da atriz Carolina Dieckmann no início deste ano. Na oportunidade, restou acordado que o atual projeto teria preferência e o anterior, do deputado Eduardo Azeredo, seria, como o fora, modificado para não tipificar qualquer conduta. Fora um fato lamentável, visto que o projeto de 1999 havia sido discutido exaustivamente e estava muito mais maduro para se tornar lei, especialmente em razão de que seu "substitutivo", o PL 2.793/11, trazia, em seu corpo, incongruências redacionais as quais seriam fonte abundante de argumentos para as defesas criminais, tornando letra morta a previsão legislativa, como por exemplo, o uso da expressão "devassar dispositivo informático". Nunca consegui entender a abrangência do verbete "devassar" com conotação demasiadamente pejorativa para um tipo penal.

A boa notícia é que o projeto foi de fato melhorado no Senado. Substituíram a expressão "devassar" por "invadir", trazendo maior clareza na conduta, bem como foram realizadas algumas correções textuais e outras adequações jurídicas, como tirar do dispositivo a previsão de obter vantagem ilícita para não prejudicar outros tipos penais, como o estelionato e o furto. Ainda, fora adequado o artigo 266 do Código Penal, colocando a tipificação no próprio *caput* e não em parágrafo, ficando agora prevista a punição a quem interrompe ou perturba serviço telemático ou dificulta seu restabelecimento.

O projeto ainda corre o risco de parar para análise conjunta ao projeto de reforma de todo o Código Penal, mas, se não for interrompido, teremos em nosso ordenamento a definição do crime de invasão de dispositivo informático, punível com detenção, de três meses a um ano, e multa, pena aplicada também a quem produz, oferece, distribui, vende ou difunde programas de computador capazes de permitir a invasão de dispositivo. Havendo prejuízo econômico, a pena é aumentada de um sexto a um terço e ainda, se da invasão forem obtidas informações sigilosas, comunicações eletrônicas privadas, segredos comerciais ou industriais, a pena será de reclusão de seis meses a dois anos, e multa. Neste caso, poderá haver acréscimo à pena se tais informações forem transmitidas a terceiros, a qualquer título. Embora apelidado de "Lei Carolina Dieckman", vejo dificuldades em se aplicar ao caso concreto da atriz, porquanto pela proposta é preciso haver: ausência de consentimento do proprietário, ainda que tácito e com a finalidade de se obter os dados. De qualquer modo, muitas outras invasões de sistemas poderãoser punidas sob a luz de tais dispositivos, tais como aquelas em que ativistas digitais retiram sites deserviço público ou governamentais do ar.

Feita essa análise do trâmite e do mérito, resta-nos refletir: o Brasil realmente precisa de uma lei que tipifique tais crimes cibernéticos? É apenas isso que nos falta?

Sendo o Brasil um país de tradições positivistas e sendo vedada a aplicação de analogia para criar tipos penais, não nos resta dúvida em responder afirmativamente a essa indagação. Especialmente para algumas condutas como a invasão de sistemas, tão específica e sem previsão semelhante no atual ordenamento. Muitos outros crimes já estão previstos e não é preciso se definir em lei que há a conduta criminosa se cometido por meio eletrônico. Talvez com a previsão dessas condutas específicas, passaremos a obter melhores resultados punitivos. Talvez (e somente talvez) em razão de que não é esse o único problema na persecução de crimes cibernéticos.

A falta de estrutura nas delegacias civis (excluo a Polícia Federal, porquanto reconhecida mundialmente pela sua competência na apuração de delitos digitais e algumas poucas delegacias especializadas em grandes centros) e a ausência de previsão legal que estabeleça a obrigatoriedade na guarda de logs acabam por inviabilizar a investigação cibernética, em muitos casos. O Marco Civil da Internet (PL 2.126/2011), embora tenha conotação civil, poderia sanar esse problema ao prever o armazenamento de tais registros, sem dar margem para violação à privacidade, evidentemente. No entanto, no último parecer de julho próximo, o relator deputado Alessandro Molon retirou a obrigatoriedade do armazenamento dos dados pelos provedores de aplicações à internet, vulgos provedores de conteúdo, deixando essa previsão apenas aos provedores de conexão. Fato é que os registros de conexão nem sempre são suficientes para uma boa colheita de provas. O certo seria obrigar também os provedores de conteúdo a fazer esse registro, permitindo, assim, não só investigar e punir os crimes previstos pelo PLC 35/2012 como também outros, tais como os de difamação, calúnia e injúria, tão comuns nas redes sociais.

Muita água irá rolar. Vamos acompanhar e torcer para que as legislações de nosso país não sejam feitas no calor das emoções e sejam refletidas em todos seus aspectos e consequências. E em conjunto com projetos e políticas públicas de estruturação das polícias técnico-científicas e também no tocante à produção de provas digitais. Crime tecnológico se combate com investimento em tecnologia. Não serão leis que tornarão o meio digital mais seguro e sim políticas públicas, desde a educação digital até o investimento em aparato investigatório.

Date Created

09/11/2012