

Os cybercrimes na esfera jurídica brasileira

Reginaldo César Pinheiro*

No final do século XIX um cidadão alemão foi preso acusado de furto de energia elétrica. Os advogados do acusado, entretanto, observaram que não existia na legislação penal alemã tal delito, pois a energia elétrica não tinha *status* de coisa, e somente coisa poderia ser passível de furto. O tribunal absolveu o réu ao entender que a lei penal não permite interpretação analógica. Com isso, o legislador alemão providenciou logo um dispositivo legal que tipificasse como crime o furto de energia elétrica, pois sem a mesma, aqueles que viessem a desviar a energia elétrica ficariam impunes.

Cerca de um século após o acontecimento noticiado pelo advogado José Henrique Moreira Lima (1), nos deparamos com um problema que em tese, é bem semelhante ao vivido pela Alemanha. Com a popularização da Internet em todo o mundo, milhares de pessoas começaram a se utilizar deste meio. Contemporaneamente se percebe que nem todos a utilizam de maneira sensata, e acreditando que a Internet é um espaço livre, acabam por exceder em suas condutas e criando novas modalidades de delito: os crimes virtuais.

Também conhecidos por Cybercrimes, estes novos delitos são interpretados, segundo a concepção do Secretário Executivo da Associação de Direito e Informática do Chile, Claudio Libano Manzur, como sendo *"todas aquellas acciones u omisiones típicas, antijurídicas y dolosas, trátese de hechos aislados o de una série de ellos, cometidos contra personas naturales o jurídicas, realizadas en uso de un sistema de tratamiento de la información y destinadas a producir un perjuicio en la víctima a través de atentados a la sana técnica informática, lo cual, generalmente, producirá de manera colateral lesiones a distintos valores jurídicos, repontándose, muchas veces, un beneficio ilícito en el agente, sea o no se caracter patrimonial, actúe con o sin ánimo de lucro."* (2) Em outras palavras: são todos os atos ilícitos praticados através da Internet que venham a causar algum tipo de dano, seja ele patrimonial ou moral, ao ofendido.

Em um primeiro momento, vem a mente de muitos aplicadores do Direito a máxima "nulla paena nulla crimen sine legge", isto é, enquanto não houver leis específicas de repressão aos crimes virtuais, não será possível que exista por parte do Estado uma atuação coercitiva eficaz. Não se pode olvidar-se, todavia, que na maioria das vezes a Internet é apenas um instrumento de ação dos cybercriminosos. Daí ser conveniente dividi-los em **crimes virtuais puros, mistos e comuns**.

Os *crimes virtuais puros*, conforme contempla o advogado Marco Aurélio Rodrigues da Costa, é "*toda e qualquer conduta ilícita que tenha por objetivo exclusivo o sistema de computador, seja pelo atentado físico ou técnico do equipamento e seus componentes, inclusive dados e sistemas.*" (3) Neste ponto é que verifica-se a ação dos *hackers*, que são pessoas com profundos conhecimentos informáticos e que se utilizam desse *know-how* para obtenção de algum benefício ilícito ou simplesmente por vandalismo. Como no caso dos ataques aos *mega-sites* ocorridos recentemente.

Por sua vez, os *crimes virtuais mistos* são aqueles em que o uso da internet é condição *sine qua non* para a efetivação da conduta, embora o bem jurídico visado seja diverso ao informático. Ocorre, por exemplo, nas transferências ilícitas de valores em uma *home-banking*.

Os *crimes virtuais comuns*, são pois, assim entendidos, porque utilizam a Internet apenas como instrumento para a realização de um delito já tipificado pela lei penal pátria. A Rede Mundial de Computadores, acaba por ser apenas mais um meio para a realização de uma conduta delituosa. Se antes, por exemplo, a pornografia infantil era instrumentalizada através de vídeos e fotografias, hodiernamente, se dá através das *home-pages*. Mudou-se a forma, mas a essência do crime permanece a mesma.

Há de se destacar, nesse contexto, as enormes dificuldades enfrentadas pelas autoridades responsáveis pela segurança no país para reprimirem este tipo de ação delituosa. Nesse sentido, o professor Antônio Scarance Fernandes assinala: "*Por enquanto a repressão se restringe ao enquadramento desse tipo de infração nos delitos tipificados pelo Código Penal*". (4) Ou seja, atualmente, somente os crimes virtuais mistos estão sendo impugnados pelo nosso ordenamento.

Em verdade, a repressão aos cybercrimes também tem encontrado barreiras referentes a conquista de provas materiais. A internet propicia, devido a sua rapidez, a possibilidade de ser eliminada a qualquer momento quaisquer vestígios necessários para a comprovação do delito. Tem-se constatado, independentemente do crime ser puro, misto ou comum, que na maioria das vezes estes delitos ainda permanecem impunes, porque ainda "*continuam a ser novidade*" para os mecanismos coercitivos estatais.

Entretanto, há uma luz ao fim do túnel, isto é, o Direito e o Estado tem trabalhado para a reversão desse quadro anárquico-cibernético. Neste aspecto, o provedor de acesso, é elemento ímpar para a corroboração da punição destes crimes. Nos furtaremos a abordar integralmente a responsabilidade do provedor, mas é importante ressaltar certos aspectos se perfazem relevantes para a tal estudo.

O provedor de acesso, salvo algumas exceções, tem interesse econômico na prestação de serviços de acesso a rede. Logo, todas as informações constantes em seu banco de dados tem alguma relevância. Quando estas informações já não são mais importantes, o provedor as elimina de seu banco de dados. Neste aspecto é que a barreiras surgem, pois independentemente do provedor ser gratuito ou não, estas informações, na maioria das vezes são elementos que comprovam tal conduta delituosa.

A polícia tem conseguido reprimir os cybercrimes se utilizando dos chamados IP (*Internet Protocol*), que identifica através do seu respectivo número a

localização do info-marginal. Neste caso o provedor de acesso é obrigado a fornecer a referidas informações para a consubstanciação da prova. Se no caso de ofensa moral a uma pessoa em uma sala de bate-papo, por exemplo, será através deste IP que poderá ser comprovado tal ofensa, para efetivação da punição *a posteriori*. Por isso se faz necessária a existência de mecanismos mais rígidos com relação as atividades do provedor de acesso, sobretudo, exigindo o armazenamento das informações de cada usuário pelo prazo de no mínimo um ano.

Por outro lado, mesmo a Internet sendo uma *Teia de Alcance Mundial*, tem as polícias conseguido punir infrações além-mar, quer dizer, os limites legislativos essencialmente territoriais tem sido superados com o apoio de polícias de outros países e também com o auxílio de organizações mundiais. Mesmo sem existir de fato um tratado internacional, algo que alguns aplicadores do Direito julgavam ser a única forma para tal repressão.

Prova disso, foi a reunião de ministros da justiça e procuradores dos países integrantes da OEA (*Organização dos Estados Americanos*) realizada em março deste ano, na qual um dos principais temas foi a criação de mecanismos para coibir a ação *hacker* na Internet. A OEA, na ocasião afirmava: "*cuidem da segurança dos sites de vocês, senão assim fica mais fácil*" (5) para os cybercriminosos. Assim, o governo brasileiro deseja, o mais depressa possível, criar uma lei que possa punir com maior rigor esses info-delitos.

Tramitam no Congresso Legislativo, por sua vez, cerca de 14 projetos de lei pertinentes aos crimes virtuais, e no entanto, é perceptível o desinteresse do governo perante a matéria. Com a pressão da OEA, porém, acredita-se que ainda este ano se terá um lei vigorando no Brasil referente aos crimes virtuais.

Dois destes projetos vem ganhando a atenção nacional. Um pertencente ao Deputado Luiz Piauhylin e outro do Senador Renan Calheiros. Ambos são vistos com ressalvas, mas entretanto, adverte o próprio senador, dizendo que "*a tipificação desse tipo de delito pelas legislações de todos os países é medida urgente e que não pode esperar mais.*" (6)

Deve-se levar em consideração sim, a urgência que se perfaz em nosso contexto, mas sobretudo, não se pode permitir que o Estado, sob o pretexto de atribuir maior segurança aos usuários da rede, viole os direitos de liberdade de expressão do cidadão. Como é o caso de art. 2.º, § 6.º, II e III, do projeto de lei do Senador Renan Calheiros, que define como crimes contra a moral pública e opção sexual, a *divulgação de material pornográfico* e a *divulgação de sons, imagens ou informação contrária aos bons costumes*, (7) respectivamente. Ora, se não se trata de pornografia infantil e nem de ofensa de privacidade, porque haveria o legislador de restringi-lo?

No espaço virtual, os defeitos e os atos ilícitos dos internautas se produzem com a mesma facilidade que no espaço real. Todavia, o Direito ao pretender tutelar o bem jurídico do cidadão precisa, necessariamente acompanhar esta evolução, a fim de possibilitar tal garantia.

Contudo, é preciso que se ampliem os debates sobre a matéria, tanto por parte do governo, quanto pela sociedade civil, no sentido de informar aos usuários sobre os novos tipos de modalidades delituosas que estes estão sujeitos, até porque, os crimes virtuais não se restringem somente a ação dos *hackers*, ela é mais ampla. A tutela do bem jurídico virtual não pode restringir-se somente à produção de legislação específica.

NOTAS

1. José Henrique Moreira Lina. *Alguns aspectos jurídicos da Internet no Brasil*. Informação obtida em: <http://www.geocities.com/CollegePark/Campus/4961/flinks.htm>.
2. Claudio Líbano Manzur. *Chile: los delitos de hacking en sus diversas manifestaciones*. In: Revista Electrónica de Derecho Informático, n. 21, Abril del 2000.
3. Marco Aurélio Rodrigues da Costa. *Crimes de informática*. In: Revista Eletrônica Jus Navigandi. Site: <http://www.jus.com.br/doutrina/crinfo.html>.
4. *Cybercrimes – legislar ou auto-regulamentar?* In: Revista RT Informa, n. 06, Março/Abril 2000, São Paulo: Editora Revista dos Tribunais, p. 04-05.
5. *Justiça vai criar comissão para punir hackers*. O Estado de São Paulo, Economia, edição de 02.03.2000, p. B6.
6. Justificação do Projeto de Lei n. 76/2000, cedido gentilmente pela assessoria parlamentar.
7. Grifos nossos.

*acadêmico de Direito da Universidade Paranaense (UNIPAR), pesquisador do Instituto de Pesquisas, Estudos e Ambiência Científica (IPEAC/UNIPAR)

PINHEIRO, Reginaldo César. Os cybercrimes na esfera jurídica brasileira . Jus Navigandi, Teresina, ano 4, n. 44, ago. 2000. Disponível em: <http://jus2.uol.com.br/doutrina/texto.asp?id=1830> Acesso em: 24 out. 2006.