Advogados pedem maior rigor para crimes cometidos através da internet

Pesquisa realizada pela fabricante de *softwares* Symantec aponta que 79% dos internautas brasileiros não acreditam que os autores de crimes praticados por meio da internet serão punidos pela Justiça. O caso do ataque ao site da Presidência da República no dia 2 de janeiro mostra que quem ataca também duvida da punição. Em entrevista ao portal *G1*, a dupla de hackers *Fatal Error Crew*, que assumiu a autoria da invasão, afirmou que não tem medo de punição, pois, no Brasil, o mundo virtual é um mundo sem leis.

Para especialistas em Direito Digital, o ordenamento jurídico brasileiro já dá conta de boa parte dos crimes eletrônicos. Porém, a pequena parcela que sobra causa a sensação de impunidade que também contribui para que mais internautas cometam delitos virtuais. Para preencher essa lacuna, foi apresentado na Câmara dos Deputados em 1999 o Projeto de Lei 84, que tipifica os crimes cometidos pela internet.

De autoria do ex-deputado Luiz Piauhylino, a proposta ficou conhecida como Lei Azeredo, em referência ao senador Eduardo Azeredo (PSDB-MG), que elaborou substitutivo à matéria no Senado. No entanto, o substitutivo teve forte rejeição política de ativistas da internet livre, que elaboraram petição online contrária à matéria intitulada "Em defesa da liberdade e do progresso do conhecimento na internet brasileira". Para piorar a situação, as divergências políticas empacaram o projeto na Câmara.

Maior rigor
Países como Chile e Argentina já possuem legislação própria. No estado da Califórnia, nos Estados Unidos, entrou em vigor em 1º de janeiro uma lei que pune internautas que criam perfis falsos na internet. A nova norma prevê multa de até US$ 1 mil ou um ano de prisão.

Para advogados ouvidos pela **Consultor Jurídico**, uma lei específica deve tratar com maior rigor esses tipos de crimes. Isso porque a legislação vigente não considerara a amplitude do prejuízo quando o crime é praticado por meio da internet. O mundo virtual é um meio facilitador de divulgação de informação, tanto na questão da quantidade de pessoas que tem acesso a elas quanto na rapidez com que se propagam.

Para o membro da Comissão de Alta Tecnologia da Ordem dos Advogados do Brasil de São Paulo (OAB-SP) **Vinícius Ravanelli Cosso**, do escritório Cosso Advogados, as penas previstas nas leis vigentes não são proporcionais ao impacto que a internet provoca. "O legislador de 1945 tinha outra noção do impacto que uma difamação teria na sociedade. Hoje, isso é exponencialmente maior com a internet, devido à velocidade e à amplitude de pessoas que podem ter acesso a essa informação. As penas deveriam ter uma valoração maior para esses casos."

Ele explicou que existe uma separação doutrinária entre crime praticado no ambiente eletrônico e crime puramente eletrônico. "Essas novas condutas devem ser tipificadas até mesmo para que as pessoas entendam que o ambiente digital não é puramente virtual na medida em que gera efeitos na vida real."

Para o presidente de Internet do Instituto Brasileiro de Política e Direito da Informática (IBDI), **Omar Kaminski**, é extremamente necessária uma lei específica, pois, na maioria das vezes, as punições

já previstas são muito baixas. "O caso do ataque ao site da Presidência pode ser enquadrado como crime de dano ao patrimônio, previsto no Código Penal, que prevê de um a seis meses de prisão, ou no artigo 10 da Lei 9.296, que trata das interceptações de comunicações telemáticas. Para esse caso, a pena é de reclusão de dois a quatro anos e multa. São punições muito baixas para o tamanho e o alcance dos prejuízos."

Ele avaliou ainda que, apesar de haver formas técnicas de se prevenir contra ataques virtuais, apenas com uma lei específica o combate a "vandalismo digital" será efetivo. "Só com a tipificação desses crimes virtuais é que a sensação de impunidade vai acabar. Mesmo porque, há casos em que quem faz isso nem sabe que pode ser responsabilizado."

Conflito de interpretação
O advogado **Rony Vainzof**, sócio do escritório Opice Blum Advogados Associados e professor em Direito Eletrônico no Mackenzie e na Escola Paulista de Direito, explicou que o ordenamento jurídico já alcança muitos crimes considerados virtuais, pois, nesses casos, virtual é o meio que se utiliza para a prática do crime, e não o crime propriamente dito.

"Não importa o meio em que se deteriora a coisa, mas sim que houve o dano. Nem todo mundo sabe disso, mas ninguém pode alegar desconhecimento da lei para se defender." Para ele, as principais condutas que não estão previstas no ordenamento jurídico são disseminar código malicioso (vírus) e invadir domicílio eletrônico.

Já o advogado **Rogério Lemos Passos Martes**, sócio do PPP Advogados e especialista em Direito Digital, lembrou que o problema de se enquadrar o ataque ao site da Presidência como dano qualificado é que o Código Penal só pode ser aplicado de acordo com que o que está escrito na lei, sem analogias. Segundo o artigo 163, causa dano aquele que destrói, inutiliza ou deteriora coisa alheia.

"O problema é que o termo ‘coisa’ trata de coisa material e o site é algo virtual. Quando o código foi implementado, não existia esse mundo digital, logo, os termos contidos nele são direcionados para o mundo real", explicou. Por isso, foi proposta a alteração do artigo 163 para incluir o temor "dano a dado eletrônico alheio". Passos Martes destacou ainda que muitos dos crimes cometidos virtualmente também geram reflexos na esfera civil, nos casos em que são pedidos indenização por dano moral ou material da vítima.

Principais ataques
De acordo com a pesquisa da Symantec, 65% da população mundial já sofreu algum ataque, sendo 51% dos casos infecções por vírus e malwares. Outros problemas frequentemente enfrentados são golpes online, com 10%, e o *phishing* — ato de enviar e-mails em nome de pessoa confiável ou empresa, com links mal intencionados —, que representa 9% das ameaças. Com 7% cada, estão o furto de perfis em redes sociais, as fraudes com cartão de crédito e o assédio sexual.

Para Passos Martes, os crimes mais comuns no país são os contra a honra, como o envio de e-mails anônimos e mensagens caluniosas ou a criação de perfis falsos em redes sociais, também chamados de furto de identidade. "Outro ponto negativo desses crimes é que, por preverem penalidade baixa, também têm um período de prescrição curto. Por isso, o mais comum é a reparação do dano por meio de

indenização ou mesmo a aplicação de penas alternativas ou suspensão do processo."

Anonimato
A dupla de hackers do *Fatal Error Crew* afirmou que atacou o site da Presidência como forma de protesto, com a intenção de passar a mensagem à população de que "votar é algo sério". Eles provavelmente se inspiraram nos hackers que atacaram em dezembro do ano passado a rede de computadores das empresas de cartões de crédito MasterCard e Visa, em retaliação ao bloqueio de doações ao site *WikiLeaks*.

Os sites das empresas foram apenas dois dos vários atacados pelo grupo *Anonymous*, que ameaçou punir as empresas que deixaram de prestar serviços ao *WikiLeaks*. O ataque foi coordenado por redes sociais, como Facebook e Twitter, além de páginas de discussão como o 4chan e redes de chat via protocolo IRC. Com isso, os pagamentos feitos por usuários da empresa de cartões de crédito foram prejudicados.

O advogado Passos Martes destacou que a dupla brasileira de hackers acabou infringindo também a Constituição. De acordo com o artigo 5º, inciso IV, da Carta Magna, é livre a manifestação do pensamento, sendo vedado o anonimato. "Usar um ato ilícito que causou prejuízos a outras pessoas não é a melhor forma de manifestação de pensamento. Pior, instiga outras pessoas a fazer o mesmo."

Identificação
Mesmo sem ter muito conhecimento técnico, qualquer um que tenha acesso à rede mundial de computadores pode praticar um crime virtual, devido à facilidade de se encontrar formas de burlar sistemas, de se criar vírus e baixar programas de invasão na internet. De acordo com Rony Vainzof, normalmente os jovens estão mais acostumados com as novas tecnologias, porém, cada vez mais criminosos "seniores" estão cooptando *hackers* para formar grupos e praticar ilícitos. "Os criminosos já perceberam que não há mais dinheiro no banco. As operações são feitas virtualmente."

Para Omar Kaminski, o ataque ao site da Presidência da República pode ser um indicativo do quanto a Polícia do país está preparada para investigar crimes eletrônicos. A Polícia Federal já anunciou que vai instaurar um inquérito para tentar identificar os responsáveis pelo ataque e verificar quais medidas podem ser tomadas contra eles.

De acordo com o *Fatal Error Crew*, para atacar o site, foi usada uma "negação de serviço", ou seja, uma criação artificial de um número elevado de solicitações simultâneas a um servidor. O golpe é similar ao utilizado para derrubar os sites da Visa e do MasterCard, com o objetivo de tornar a página indisponível. Kaminski acredita que existe a possibilidade de os *hackers* serem identificados, apesar de o tipo de ataque aplicado dificultar a identificação de sua origem, uma vez que os criminosos podem forjar o endereço de onde saiu o ataque. O advogado destacou ainda que o ataque também é importante, pois poucos são os casos de crimes eletrônicos de grande repercussão no país. "Ou a investigação desses crimes não é divulgada ou está se dando pouca importância para isso, o que é muito grave."

O levantamento da Symantec mostrou que 76% dos brasileiros adultos que utilizam a internet já foram vítimas de algum crime digital. O Brasil está empatado com a Índia, superando os Estados Unidos, com 73%, e ficando atrás apenas da China, com 83%. Para Vaizonf, apesar de a internet dar a sensação de anonimato, todas as ações do internauta deixam um registro. "Esse tipo de ataque, que utilizou um

conjunto maciço de informações enviadas de vários computadores zumbis [*raqueados*], torna a investigação mais difícil, mas não impossível, pois sempre fica um rastro. Dentro da área da tecnologia, é impossível ter 100% de segurança. Novos ataques sempre aparecem."

Já para o advogado Vinícius Cosso, a identificação do *hacker* depende de sua competência técnica e de como é feita a proteção do sistema invadido. "Antigamente, alguns *hackers* apagavam o registro da sua invasão. Mas quando o operador do sistema verificava que algo foi apagado, ele automaticamente entendia que houve uma invasão." Cosso afirmou ainda que há um sistema de proteção que imprime todos os registros do sistema. Dessa forma, mesmo se algum registro for apagado, ainda há a prova em papel. No entanto, esse sistema é pouco utilizado hoje em dia. Atualmente, são mais utilizados sistemas paralelos.

Tramitação
O Projeto de Lei 84/99 foi aprovado pela Câmara em 2003 e voltou do Senado em 2008. Apesar de tramitar em regime de urgência, as comissões que tratam do tema não chegaram a votar seus pareceres. O ponto mais polêmico do texto é a obrigatoriedade de os provedores armazenarem por até três anos as informações de conexão dos usuários.

O substitutivo apresentado em novembro de 2010 pelo relator do projeto na Comissão de Constituição e Justiça e de Cidadania (CCJ), deputado Regis de Oliveira (PSC-SP), obriga provedores de acesso e de conteúdo a armazenar informações como IP (número que identifica uma conexão à internet), data e hora da conexão.

A versão do senador Eduardo Azeredo determina essa obrigação apenas aos provedores de acesso. Consta também do texto que partiu do Senado a tipificação das condutas a serem consideradas crimes digitais, como disseminação de código malicioso e distribuição de informações sigilosas.

Date Created
08/01/2011