INTERNET

Tecnologia a serviço do crime

Se alguém invadir remotamente seu computador e apagar todos os seus arquivos, nenhum crime terá sido cometido, segundo as leis brasileiras. In vasões, vírus de computador, destruição de dados e novas formas de condutas abusivas uniram-se a delitos "clássicos" como pedofilia, racismo e violência moral no ciberespaço, em prejuízo da vida das pessoas no mundo real. Os invasores são conhecidos popularmente como *hackers*, mas há controvérsias quanto a essa qualificação pois alguns consideram que o termo *cracker* define melhor os invasores (veja box). Se no início da internet os *hackers* foram vistos com simpatia, por sua esperteza e sagacidade, atualmente são encarados como criminosos. "Os danos são cada vez maiores diante da forte dependência tecnológica existente hoje na estrutura produtiva da sociedade", diz o advogado especialista em direito cibernético Rodrigo Guimarães Colares, do escritório Martorelli e Gouveia. "Se você usa a internet, o risco de ser vítima de um crime tecnológico sempre existe".

Colares classifica os crimes tecnológicos em duas categorias. A primeira inclui crimes tradicionais que utilizam a internet como meio para sua prática: casos de pedofilia, ofensas morais, racismo, plágio e incitação à violência. A estas ações , o especialista dá o nome de "crimes eletrônicos". Na segunda categoria estariam as práticas ofensivas cujo fim é a lesão a dados ou sistemas computacionais, especialidade dos *hackers*. São os crimes chamados "informáticos", que na maioria das vezes não têm previsão em lei no Brasil e, portanto, a rigor, não podem ser chamados de "crimes" no sentido jurídico da palavra, diferentemente do que ocorre em outros lugares do mundo.

Além de uma infinidade de sites e *blogs* destinados aos crimes eletrônicos, há o uso de sites derelacionamento, como o Orkut, para essas práticas ilegais. A polêmica envolvendo o Orkut está na omissão de seus gestores (a gigante Google) diante da incitação a ações criminosas, praticadas por usuários que criam perfis falsos (*fake*) para agir. "Esse é o grande trunfo dos criminosos", afirma o advogado Márcio Benjamin, do escritório Costa Barros Associados. "Mesmo que se consiga identificar o computador de onde partem os delitos pelo endereço IP [número único que identifica cada computador conectado à internet], é impossível afirmar com certeza quem é o usuário que praticou o dano, sobretudo quando as ações partem de computadores localizados em *lan-houses* [casas de jogos de computadores e internet]", diz Benjamim.

Entre as invasões e alterações ilegais nos sistemas informáticos de cidadãos e empresas, destacam-se roubo de senhas e informações sigilosas para fraudes financeiras, corrupção de arquivos e páginas da internet e, ainda, seqüestro de documentos importantes (seguido do pedido de altas somas em dinheiro para o resgate). No que diz respeito às fraudes financeiras, em 2005 houve no país um aumento de 579% com relação a 2004, segundo levantamento do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (Cert.br).

O QUE DIZ A LEI Ainda não há uma legislação específica para crimes tecnológicos no Brasil. Até o momento, houve algumas tentativas em se criar uma lei de crimes informáticos, sem qualquer resultado efetivo, salvo adaptações pontuais no Código Penal. O primeiro Projeto de Lei (PL 84/99), de autoria do deputado Luiz Piauhylino (PDT/PE), tipifica os crimes praticados eletronicamente e inclui novas modalidades de crimes, como o acesso indevido a meios eletrônicos e a difusão de vírus computacionais. "As novas modalidades de crimes (crimes informáticos) não estão previstas no Código Penal, criado em 1940, quando não existia nem computador", diz Colares.

O PL 84/99 foi substituído pelo PL 89/2003 e incorporado à proposta do senador Eduardo Azeredo, junta-

mente com os PLs 76/2000, do senador Renan Calheiros (PMDB/ AL) e 137/2000, do senador Leomar Quintanilha (PCdoB/TO). O novo projeto de lei propõe a identificação obrigatória dos usuários da internet antes de iniciarem qualquer operação que envolva interatividade, como o envio de e-mails, conversa em salas de bate-papo, criação de *blogs* e captura de dados (*download* - baixar músicas, filmes, imagens etc). O acesso sem prévia identificação seria punido com reclusão de dois a quatro anos. Os provedores teriam a responsabilidade pela veracidade dos dados cadastrais dos usuários e estariam sujeitos à mesma pena caso se permitisse o acesso de usuários não-cadastrados.

Bancos, organizações não-governamentais (ONGs), provedores de acesso e advogados discutem o PL sobre cibercrimes mas não há consenso. Permitir o avanço de investigações policiais por meio do rastreamento é o grande argumento dos defensores do PL. Porém, a efetividade da prevenção dos crimes é questionada devido à possibilidade de acesso à internet por provedores de outros países (portanto, não submetidos às leis brasileiras). Há ainda o argumento de que, quando o objetivo é impedir crimes eletrônicos, o controle deveria ser feito na inserção do conteúdo, e não no acesso. A crítica geral dos opositores ao projeto é de que a medida irá provocar a burocratização do acesso e a perda de privacidade dos usuários.

O conteúdo do projeto de Azeredo segue definições estabelecidas internacionalmente pela Convenção de Budapeste (de 2001), ratificada por 43 países da Comunidade Européia e pelos Estados Unidos, em vigor a partir de 2007. A Convenção autoriza o monitoramento das ações eletrônicas dos usuários da internet, mas muitos países ainda não a ratificaram, entre os quais os países do Reino Unido, Portugal, Espanha e Itália. "Uma resolução como essa pode até ser interessante para países que convivem com ameaças terroristas, mas não deixa de ser uma forma de invasão de privacidade", afirma Colares.

Flávia Gouveia

Glossário Hacker

CAVALO-DE-TRÓIA programa disfarçado com arquivo anexado que possibilita a entrada do hacker.

CRACKER são os hackers mais radicais. Eles pirateiam programas e penetram em sistemas "quebrando" tudo. A intenção é sabotar ao máximo os grandes servidores.

DEFACER usuário mal-intencionado que passa o tempo tentando desfigurar a página inicial de sites conhecidos.

FIREWALL PESSOAL software que impede usuários não autorizados de acessar um PC isolado.

HACKER a palavra surgiu nos anos 50 dentro do MIT e deriva do termo *hack*, usada para definir atividades de alta tecnologia com os quais alguns estudantes se ocupavam. Alguém que, deliberadamente, ganha acesso a outros computadores, freqüentemente sem conhecimento ou permissão do usuário.

PHISHING SCAMS um e-mail disfarçado que tenta enganar usuários com sites falsos e promessas infundadas. Geralmente são cópias quase idênticas de páginas de bancos que levam os internautas a digitar suas senhas e números de cartão de crédito.

PORTA conexão eletrônica que permite que os dados trafeguem entre um PC cliente e um servidor através de uma rede.

VARREDURA DE PORTA (SCAN): dados enviados por um hacker para localizar um PC ou uma rede e descobrir se há portas abertas que aceitem a conexão.

Para saber mais: *http://br.geocities.com/webdesign_nit/hacker.html*