HACKERS, CRAKERS E SPAMMERS: QUEM SÃO E O QUE FAZEM?

Sérgio Gonçalves

sergio.goncalves@clgadvogados.com.br

Data criação: 22.07.2001
Data publicação: 03.12.2001

Primeiro é necessário dizer-se quem são “Hackers” e “Crackers”. Os verdadeiros “Hackers” eram especialistas em informática que estudavam ou trabalhavam com computadores, em especial nos Estados Unidos. Hoje, grande parte dos “Hackers” originais ou trabalha na área de segurança de computadores para grandes empresas e até para governos. Em Israel os “Hackers” pegos podem escolher: se trabalharem para o governo ficam livres e, em caso de recusa, vão para a cadeia. Na realidade, perigoso mesmo é o “Cracker”, pois é ele quem é invade sistemas (hardware e softwares) com o intuito de causar danos ou obter vantagens financeiras. No campo das denominações, há ainda o “Carder”, que é aquele que falsifica e opera com cartões de crédito, o “Phreaker”, especializado em delitos envolvendo telefonia e muitos outros, identificados de acordo com sua área de atuação. Porém, convencionou-se na mídia que todos são “Hackers” e assim vamos tratá-los neste artigo.

A quase totalidade dos “pseudo-hackers” que atrapalham a Internet hoje são jovens entre 14 e 20 anos, que estudam, não trabalham ou tem ocupações que envolvem informática e tem acesso a um computador de onde resolvem manifestar sua rebeldia, entrando em computadores alheios para, quando não roubar, destruir arquivos. Citando os ensinamentos de Salvatore Ardizzone, professor efetivo de Direito Penal na Universidade de Palermo na Itália, há dois grupos básicos de danos causados pelos “Hackers”: danos e condutas lesivas praticadas no computador, ou seja, danos, relativos aos suportes físicos (hardware) e alterações dos programas (software) e danos praticados através do computador, no caso de ofensa a bens da pessoa ou a interesse Públicos.

Basicamente temos que as condutas dos criminosos da informática podem ser resumidas em sabotagem, acesso ilegal, violações de segredo informático e do sigilo, falsificações, fraude informática e a violação dos direitos do autor concernentes ao software. Há ainda outras condutas que podem ser causadoras de prejuízos para empresas e demais instituições, como o furto de tempo, que consiste em uso do computador fora do propósito pelo qual se tem acesso ao equipamento, seja esta conduta motivada por fins de lucro ou apenas por passatempo. O que importa dizer é que para cada um destes comportamentos devemos associar ao fato (ou ao seu resultado), o caminho legal necessário para não só parar a conduta lesiva, como para responsabilizar seu autor civilmente pelos danos que haja causado. As legislações específicas sobre as condutas no meio virtual são muito mais voltadas, nos dias de hoje, para a área penal, restando para a reparação cível dos danos, no mais das vezes, socorro em na legislação existente. Entretanto isto não chega a ser um problema, uma vez que em havendo prejuízo na esfera material ou pessoal, isto basta para que os meios processuais atuais possam ser buscados para responsabilizar civilmente os “Hackers”.

Dependendo da conduta praticada pelo autor, seja ele hacker ou uma pessoa comum, torna-se difícil sua responsabilização. É o caso dos “Spammers” ou seja, quem se utiliza do “Spam”, que é o envio de mensagens não autorizadas, em geral comerciais, através de e-mails. Não há em nosso país, ao contrário dos Estados Unidos, por exemplo, nenhuma legislação em vigor que trate deste tipo de problema. O “Spam” em si, na sua forma mais comum, pode trazer como único prejuízo ao usuário um maior gasto com a conexão necessária para se receber e ler as mensagens e um dispêndio maior de tempo para esta tarefa. Porém, o abuso na

quantidade de e-mails enviados, pode caracterizar ilícito civil (art. 159 do CC), desde que provados danos materiais ou morais, da mesma forma que com relação a qualquer correspondência, ainda mais se o endereço do destinatário não foi obtido dele próprio ou de listagem pública. Os danos surgidos nestas hipóteses, morais ou materiais, podem ser objeto de ações indenizatórias, até mesmo contra empresas nas quais trabalhe o ofensor.

O maior problema, no entanto, é encontrar quem responsabilizar de fato e comprovar, em juízo, todas as circunstâncias envolvidas neste tipo de situação, demonstrando o prejuízo sofrido. As condutas podem ser praticadas fora do território de um país e lá produzir resultados, o que faz com seja necessário, em um futuro não muito distante, encontrar meios de fazer valer leis de proteção aos delitos digitais de um modo global e com processos mais rápidos que os tradicionais. Este, é o maior desafio jurídico que a rede nos apresenta para ser resolvido e que, ao que parece, continuará por um bom tempo sem resposta.

Sérgio Gonçalves é advogado e conferencista, sócio da Correia Lopes e Gonçalves Advogados Associados (CLG Advogados), especialista em Direito Civil e Direito Eletrônico. Fundador e editor do Informativo Jurídico "O Neófito. Professor em curso de Pós-graduação em Direito de Informática, conselheiro do Instituto Brasileiro de Política e Direito de Informática (IBDI), do Centro de Estudos Tributários e Empresariais (CETE) e conselheiro-convidado da Organização das Nações Unidas Brasil. É também autor de diversos artigos sobre Direito Internacional, Empresarial, do Consumidor e Direito Eletrônico publicados em revistas, jornais e websites. Colunista do jornal Gazeta Mercantil sobre Direito Empresarial e co-autor dos livros "Comércio Eletrônico" (Editora Revista dos Tribunais) e "Direito Eletrônico - A Internet e os Tribunais" (Edipro).