# Responsabilidade por crime eletrônico chega às empresas

Os recentes pedidos de quebra de sigilo de dados de usuários do site de relacionamento Orkut, de responsabilidade do Google, inflamaram ainda mais a polêmica que envolve o mundo corporativo e jurídico, especificamente no que toca à responsabilidade das empresas e seus dirigentes pelos atos praticados por seus funcionários.

É cada vez mais comum casos de funcionários de empresas utilizarem-se dos instrumentos de trabalho oferecidos pela companhia, como acesso à internet e e-mail, para o cometimento de crimes, em sua maioria de natureza patrimonial, comumente denominado de furto eletrônico, estendendo-se a outros crimes, tais como injúria, difamação, calúnia, racismo e pedofilia. Daí surge a questão: a empresa e seus dirigentes são responsáveis penal e civilmente por esses crimes ?

A questão é controvertida, pois envolve situação nova para o mundo jurídico, vez que abarca o denominado crime eletrônico. Para uns, incluindo a autora do presente, trata-se do mesmo crime tipificado no Código Penal, porém praticado em um novo meio, o eletrônico, até então desconhecido. Para outros, entretanto, trata-se de um crime novo, não tipificado em nosso Código Penal, portanto passando à margem de qualquer punição.

Nosso objetivo é alertar as empresas do risco que correm ao não se atentarem para a prevenção básica do crime eletrônico, pois as falhas de segurança nos sites e programas de acesso à internet são as grandes responsáveis por viabilizar este tipo de crime o que, em última análise, acaba por gerar além de outros inconvenientes, contingência para as empresas. Isto porque há quem atribua responsabilidade por esses ilícitos às empresas e seus dirigentes por entenderem que estes dão condições para que o crime seja cometido ou seu autor não encontrado.

Os comentários acima, aliados aos recursos técnicos existentes que permitem a identificação do computador de onde foi cometido o crime, por meio de perícia técnica e simples consulta ao site www.registro.br, onde são registrados todos os denominados IPs e seus respectivos proprietários, passam a dar suporte à extensão da responsabilidade, inclusive criminal, ainda que erroneamente, para os empresários que, supostamente, de maneira indireta, proporcionaram os meios para a prática do crime eletrônico em si.

Temos assistido à intimação de empresas, na pessoa de seus representantes legais, para prestarem esclarecimentos junto às autoridades competentes a respeito de furtos eletrônicos, com base na identificação do número do IP registrado em nome da empresa perante o www.registro.br de onde a mensagem criminosa foi originada.

Daí começam os inconvenientes. Em geral, as empresas ainda não se atentaram para a necessidade de manter um rígido controle sobre os usuários de cada IP e em situação semelhante à descrita, caso o depoimento à autoridade policial implique na impossibilidade de identificar-se precisamente o autor do furto eletrônico, referida autoridade tem adotado entendimento no sentido de que a responsabilidade deva recair sobre seus dirigentes.

É bem verdade que, em se tratando de responsabilidade civil advinda de tal conduta, esta pode derivar, dependendo do caso e de sua condução, de duas vertentes legais: a primeira, do ilícito penal, que traz no campo do direito civil a obrigação de indenizar por atos ilícitos; e a segunda, da responsabilidade extracontratual por danos causados a terceiros como conseqüência do mau funcionamento da empresa e danos causados pelos empregados quando realizam trabalho em seu nome, seja interna ou externamente.

Dada a importância do assunto e a necessidade imediata da tomada de medidas internas pelas empresas para minimizar os crimes eletrônicos, o grupo norte-americano de segurança na internet Cert em conjunto com o Serviço Secreto dos Estados Unidos e a revista CSO apresentaram recentemente uma pesquisa indicando as melhores maneiras de evitar o crime cibernético dentro das empresas[1].

O estudo envolveu 500 participantes, que elegeram as dez maneiras mais eficientes para o combate e prevenção aos crimes praticados na internet, que listamos abaixo:

1 – Empregar um funcionário dentro da empresa para monitoramento de conteúdo;

2 – Elaborar, por escrito, uma política para práticas inapropriadas;

3 – Solicitar aos funcionários que assinem um termo de compromisso às políticas implementadas;

4 – Monitorar conexões com a internet;

5 – Elaboração periódica de relatórios sobre uso inapropriado e abuso dos meios eletrônicos da empresa;

6 – Criar programas para educação e conscientização de funcionários quanto ao crime eletrônico;

7 – Desenvolver uma política de segurança corporativa;

8 – Criar programas para educação de novos funcionários;

9 – Promover avaliações de risco periódicas;

10 – Conduzir auditorias de segurança periódicas dentro da empresa.

Ressalte-se que o perigo de que ora se trata não se restringe às chamadas empresas virtuais. Ele é constante para todas as empresas que possuem rede de internet e disponibilizam e-mail aos seus funcionários independentemente do produto ou serviço vendido ou mesmo de seu porte. Assim, é importante que todos se conscientizem de que se trata de mais uma assunção de responsabilidade pelas empresas que deve ser contingenciada quando necessário, seja em decorrência dos gastos com a prevenção, seja por conta da possível condenação em processos indenizatórios por falta de prevenção.

**Nota de rodapé**

1 – Informação obtida no site www.apoioti.com.br.

**Date Created**
04/01/2007