



EUA: obtenção de dados por espões pode virar crime

Advogados dos Estados Unidos buscam formas inovadoras de enquadrar na legislação um crime novo conhecido como “pretexting” e que tem o sinônimo de “engenharia social”. Pretexting pode ser livremente traduzido como “fingimento”. O colunista Kevin Fayle, do site *Findlaw*, explica que “pretexting essencialmente envolve uma pessoa, que contacta uma companhia e finge ser algo que não é para poder obter informações de alguém em particular”.

Ele destaca que o recente escândalo das empresas HP “mostra como as companhias têm usado o pretexting, envolvendo investigadores particulares, para sondar diretores das empresas que obviamente pagaram esses investigadores”. A HP é acusada de ter contratado investigadores, pela técnica de “pretexting”, para checar onde haveria vazamento de informações a partir do conselho executivo da empresa.

O escândalo de espionagem no caso da HP gerou a demissão da presidente do conselho de administração e de um dos diretores. A sede da empresa viveu dias tumultuados desde que se tornou público o escândalo de espionagem, que envolveu investigadores particulares e métodos de vigilância em busca de uma fonte que estaria vazando informações para a imprensa.

As demissões aconteceram depois que detetives particulares que investigavam vazamentos de informação ultrapassaram os limites. Eles teriam utilizado dados pessoais dos diretores da empresa para obter registros detalhados de ligações feitas por eles e identificar quais deles estavam falando com a imprensa e passando informação. A presidente do conselho à época, Patricia Dunn, justificou a necessidade da investigação afirmando que a empresa deve zelar pela informação que chega ao público.

O colunista aponta que o pretexting “é uma maneira simples, de baixa tecnologia e assustadoramente comum que cavadores de novidades e dados, investigadores particulares, têm usado para ganhar acesso a informações pessoais”.

Para Fayle, “esse fingidor (pretexter) tentará ser um cliente, um repórter ou um membro da família”. Ele explica que esse tipo de assertiva de espões “tem sido muitíssimo usado para se obter dados de empresas de telecomunicações, como por exemplo registros de chamadas telefônicas ou de membros da família”. Fayle diz que nos Estados Unidos existem grandes corporações que sobrevivem vendendo mão de obra para trabalhos de pretexting.

Regras

A procuradoria-geral de Justiça da Califórnia, a Procuradoria da República, o FBI, a polícia federal americana, o Comitê de Energia e Comunicações do Estado e agora os advogados dos investigados pela HP buscam formas de enquadrar o crime de “pretexting” na legislação.

Agora, há a tentativa de se enquadrar o crime no Ato e Gramm-Leach-Bliley (artigo 15 U.S.C. parágrafo 6.821 a 6.827). O “pretexting” seria enquadrado como um crime de serviços financeiros. “O que é interessante disso é que apesar de ser ilegal obter dados via pretexting, não é correntemente ilegal vender



esses dados, uma vez obtidos”, observa o colunista.

Um projeto de lei apresentado pelo senador Charles Schumer propõe que ambas as práticas, obtenção e venda de dados, sejam reputadas ilegais.

Especificamente na Califórnia, o “pretexting” pode ser punido por lei que penaliza acessos desautorizados a dados de computador. O Código Penal do estado, em sua seção 530.5, torna crime o ato de se obter informações pessoais para fins ilegais.

Visite o blog [Consultor Jurídico nas Eleições 2006](#).

Date Created

14/09/2006