EUA: obtenÃ§Ã£o de dados por espiÃµes pode virar crime

Advogados dos Estados Unidos buscam formas inovadoras de enquadrar na legislaÃ§Ã£o um crime novo conhecido como â??pretextingâ?• e que tem o sinÃ´nimo 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 nÃ£o Ã© para poder obter informaÃ§Ãµes de alguÃ©m em particular”.

Ele destaca que o recente escÃ¢ndalo das empresas HP “mostra como as companhias tÃªm usado o pretexting, envolvendo investigadores particulares, para sondar diretores das empresas que obviamente pagaram esses investigadores”. A HP Ã© acusada de ter contratado investigadores, pela tÃ©cnica de “pretexting”, para checar onde haveria vazamento de informaÃ§Ãµes a partir do conselho executivo da empresa.

O escÃ¢ndalo de espionagem no caso da HP gerou a demissÃ£o da presidente do conselho de administraÃ§Ã£o e de um dos diretores. A sede da empresa viveu dias tumultuados desde que se tornou pÃºblico o escÃ¢ndalo de espionagem, que envolveu investigadores particulares e mÃ©todos de vigilÃ¢ncia em busca de uma fonte que estaria vazando informaÃ§Ãµes para a imprensa.

As demissÃµes aconteceram depois que detetives particulares que investigavam vazamentos de informaÃ§Ã£o ultrapassaram os limites. Eles teriam utilizado dados pessoais dos diretores da empresa para obter registros detalhados de ligaÃ§Ãµes feitas por eles e identificar quais deles estavam falando com a imprensa e passando informaÃ§Ã£o. A presidente do conselho Ã Ã©poca, Patricia Dunn, justificou a necessidade da investigaÃ§Ã£o afirmando que a empresa deve zelar pela informaÃ§Ã£o que chega ao pÃºblico.

O colunista aponta que o pretexting “Ã© uma maneira simples, de baixa tecnologia e assustadoramente comum que cavadores de novidades e dados, investigadores particulares, tÃªm usado para ganhar acesso a informaÃ§Ãµes pessoais”.

Para Fayle, “esse fingidor (pretexter) tentarÃ¡ ser um cliente, um repÃ³rter ou um membro da famÃlia”. Ele explica que esse tipo de assertiva de espiÃµes “tem sido muitÃsimo usado para se obter dados de empresas de telecomunicaÃ§Ãµes, como por exemplo registros de chamadas telefÃ´nicas ou de membros da famÃlia”. Fayle diz que nos Estados Unidos existem grandes corporaÃ§Ãµes que sobrevivem vendendo mÃ£o de obra para trabalhos de pretexting.

Regras

A procuradoria-geral de JustiÃ§a da CalifÃ³rnia, a Procuradoria da RepÃºblica, o FBI, a polÃcia federal americana, o ComitÃª de Energia e ComunicaÃ§Ãµes do Estado e agora os advogados dos investigados pela HP buscam formas de enquadrar o crime de “pretexting” na legislaÃ§Ã£o.

Agora, hÃ¡ a tentativa de se enquadrar o crime no Ato e Gramm-Leach-Bliley (artigo 15 U.S.C. parÃ¡grafo 6.821 a 6.827). O “pretexting” seria enquadrado como um crime de serviÃ§os financeiros.

“O que Ã© interessante disso Ã© que apesar de ser ilegal obter dados via pretexting, nÃ£o Ã© correntemente ilegal vender esses dados, uma vez obtidos”, observa o colunista.

Um projeto de lei apresentado pelo senador Charles Schumer propÃµe que ambas as prÃ¡ticas, obtenÃ§Ã£o e venda de dados, sejam reputadas ilegais.

Especificamente na CalifÃ³rnia, o “pretexting” pode ser punido por lei que penaliza acessos desautorizados a dados de computador. O CÃ³digo Penal do estado, em sua seÃ§Ã£o 530.5, torna crime o ato de se obter informaÃ§Ãµes pessoais para fins ilegais.

*Visite o blog **Consultor JurÃdico nas EleiÃ§Ãµes 2006**.*