Advogados esclarecem limites de investigações cibernéticas de funcionários

Crimes virtuais, fraudes internas, apropriação indevida. Esses são alguns dos problemas que assustam desde os pequenos empresários até as maiores empresas de tecnologia. Os chamados crimes cibernéticos, praticados por hackers, exigem investigações por parte da empresa atacada que, se não forem feitas com cuidado, podem atingir o direito à privacidade e violar o sigilo do empregado.

Por ser recente e cada vez mais criativo, esse tipo de crime ainda é motivo de dúvidas não só para empresas, mas também para advogados e juízes. O assunto foi discutido durante evento sobre o combate e prevenção a crimes digitais promovido pela empresa Kroll e o escritório Pinheiro Neto Advogados, nesta sexta-feira (11/4). A discussão foi mediada pela diretora associada da Kroll para divisão de investigações, Snezana Petreska, e contou com a participação dos diretores da empresa, Robert Brenner e Alan Brill.

Segundo **Alan Brill**, um dos fundadores das áreas de investigações da Kroll, nos Estados Unidos, aqueles que têm expertise no assunto estão ajudando os juízes na interpretação dos problemas cibernéticos. Esses profissionais dão explicações imparciais relevantes para o juiz entender e decidir no caso específico.

Brill afirma que a necessidade desses conhecimentos está aumentando. Empresas de vários setores buscam profissionais que saibam lidar com crimes cibernéticos já que, ainda que os problemas sejam particulares de cada lugar, as soluções e as regras a serem seguidas são as mesmas. O desafio é encontras soluções únicas usando as evidências particulares de cada empresa.

Os problemas mais frequentes acontecem na área trabalhista e geram questionamentos ainda sem respostas consolidadas pela Justiça, como por exemplo: a empresa pode acessar o e-mail coorporativo do empregado? Informações deletadas do computador usado pelo empregado na empresa podem ser usadas como evidências em casos de fraude? Ou ainda: as conversas que acontecem por meio de computadores dos empregados podem ser monitoradas?

Em primeiro lugar, Brill orienta as empresas a revisar os contratos feitos com os empregados para que eles estejam cientes das políticas internas — inclusive quanto à parte que fala dos equipamentos fornecidos ao empregado, como computadores e celulares, e que podem ser usadas como provas em casos de fraude. “Uma simples mudança no contrato ou uma notificação podem evitar que a empresa tenha o material, mas não possa usá-lo em juízo. Essa surpresa negativa pode ser evitada se as políticas da empresa foram revisadas antes de o crime acontecer”, afirmou.

Em relação aos equipamentos entregues aos funcionários, a Justiça tem entendido que, se a empresa está fornecendo computadores, disco rígido e celular, esses materiais são de propriedade da empresa e as informações contidas neles podem ser usadas durante uma investigação.

Um dos poucos temas consolidados pela Justiça é sobre o e-mail coorporativo. Nesse caso, a empresa

pode monitorar o uso das contas abertas para os funcionários, porque ela corre o risco de ser responsabilizada na hipótese de alguma atitude ilegal. Por exemplo, se o funcionário tem acesso a pornografia infantil no seu computador do trabalho. O armazenamento dessa informação dentro da rede já pode causar problemas de natureza criminal para a companhia, como explica **Marcos Masenello Restrepo**, do Pinheiro Neto Advogados.

Segundo ele, pelo fato de a empresa ser proprietária dos bens, ela tem direito de administrar e supervisionar seu uso. “Além disso, ela tem o interesse jurídico legítimo de garantir que eles estejam sendo utilizados de forma apropriada”, afirmou. De acordo com o advogado, a jurisprudência entende que a política da empresa é um requisito para permitir o acesso à informação.

Restrepo afirma que, no caso do computador da empresa e do e-mail coorporativo, se o empregado for informado sobre a política da empresa, ele sabe que não está recebendo os materiais para uso privado, mas para o trabalho. O advogado faz uma analogia com a correspondência. Se o empregado receber uma carta do banco, por exemplo, com o nome dele, mas no endereço da empresa, esse é claramente um material privado, de interesse pessoal. Mas se a carta vier com o nome da empresa e dizendo: “aos cuidados do empregado”, essa é uma correspondência comercial “e não haveria a violação de privacidade se alguém da empresa a abrisse, porque a carta foi enviada ao determinado funcionário não como indivíduo particular, mas como funcionário da empresa responsável por aquele assunto”, afirma.

Entretanto, as empresas encontram limitações quando se trata de informações particulares dos funcionários. Se durante uma investigação de irregularidade a empresa encontra um e-mail do empregado que pode causar algum constrangimento a ele, Restrepo orienta que a companhia não leia e nem repasse a informação, porque, ainda que a empresa tenha o direito de acesso àquele e-mail, a divulgação de informações privadas, que nada têm a ver com a atividade profissional, pode criar uma responsabilização por violação do sigilo do funcionário.

Informações deletadas

As conversas, e-mails e documentos que foram deletados de um computador ainda podem ser usadas como provas numa investigação. Isso porque, segundo o advogado, as informações apagadas continuam no disco rígido do computador e, na análise dos conteúdos da máquinas, elas podem ser resgatadas e usadas como evidências, já que estão no computador da empresa.

Segundo Restrepo, quando o usuário apaga algum conteúdo do computador, o espaço em que a informação deletada fica disponível até ser usado novamente — o que, em muitos casos, nunca acontece devido ao tamanho da memória do computador.

Mas o uso dessas informações também encontra limitações. Elas só podem ser usadas se forem pertinentes ao objeto da investigação e se não forem totalmente voltadas para a vida particular do empregado.

Invasão de privacidade
Nesse cenário, os funcionários podem usar o argumento de invasão de privacidade. Entretanto, segundo Restrepo, a jurisprudência já restringiu muito os casos em que esse argumento é válido quando se tratade material da empresa.

Questão difícil é em relação a documentos particulares abertos no computador ou celular da empresa. O advogado cita o exemplo do empregado que acessa o site do banco dele na empresa. Ainda que ele não salve nada no computador, o acesso gera uma cópia virtual na máquina que pode ser recuperada caso necessário. Esse tipo de informação, segundo ele, além do direito a privacidade, envolve o sigilo de informações bancárias e, portanto, deve ser usado com cuidado.

Mesmo assim, ele entende que o próprio acesso à informação não é ilegal, uma vez que a empresa só vai saber qual é essa informação depois de examiná-la. “Não é o caso de sigilo bancário, porque a empresa não está acessando a informação pelo site do banco, e nem usando a senha do funcionário para acessar a conta. Está apenas examinando o documento porque ele foi arquivado no computador da empresa.” Entretanto, ele ressalva que a admissibilidade dessa informação pode ser discutida em juízo.

Conversas monitoradas
A jurisprudência entende que a empresa não pode fazer o monitoramento da conversa via e-mail, porque, de acordo com Restrepo seria o equivalente a uma interceptação telefônica. Mas, se o empregado acessou o e-mail particular e baixou um documento no computador da empresa, esse pode ser analisado e não haverá violação de correspondência. Nesse caso, o advogado também afirma que o material pode não ser admitido como prova por violação de sigilo ou de direito a privacidade.

Date Created
12/04/2014