Opinião: Fator humano é o maior desafio para informações sigilosas

Em uma época em que muito se fala no valor dos dados e na sua devida proteção, onde alguns até arriscam a considerar, sob o prisma do valor econômico, os dados como o novo petróleo para a sociedade, as informações corporativas também passam a ter cada vez mais valor, sendo, por muitas vezes, ativos mais relevantes do que os próprios bens tangíveis (dinheiro, móveis, dispositivos eletrônicos e etc. de uma companhia.

Por um bom tempo, as empresas tiveram como linha de frente, na atuação de segurança da informação, a proteção de suas informações em face de ataques e invasões externas, investindo em ferramentas tecnológicas de ponta para tanto. Entretanto, com as constantes alterações nas formas de trabalho e do próprio ambiente de trabalho cada vez mais digital e conectado, as empresas vislumbraram a extrema importância da implantação de sistemas de segurança que monitorem o curso e o ciclo das informações dentro das instituições, bem como mitiguem riscos de eventuais vazamentos para o ambiente externo, o que acarreta prejuízos imensuráveis e, por vezes, irreversíveis.

Nesse passo, atualmente uma das grandes preocupações das empresas está no desvio de arquivos e informações sigilosas pelos próprios colaboradores, os quais possuem amplo acesso a dados extremamente sigilosos e valiosos, tais como estratégias de vendas, nomes de clientes, lançamento de novos produtos e preços praticados no mercado. É o fator humano como um dos grandes riscos para a segurança cibernética das empresas.

Assim, muitas companhias buscam conscientizar seus funcionários por meio de cursos, treinamentos ou códigos de conduta, porém, não raro, colaboradores acabam por desviar informações sigilosas para seus e-mails pessoais e/ou armazenam os documentos em dispositivos removíveis, como *pen drives* ou cartões SD, ou ainda armazenam os documentos em serviços de nuvem, com os mais diversos objetivos.

Sem falar na chamada Shadow IT, ou seja, os sistemas de tecnologia da informação e soluções de nuvem construídas e usadas dentro das organizações[1] sem a aprovação expressa para acessar e manipular dados da empresa, fugindo do controle prático das áreas responsáveis pela segurança das informações, constituindo, portanto, uma porta de acesso para ataques e incidentes de vazamentos de dados.[2]

Em recente pesquisa[3], mostrou-se que cerca de 46% dos incidentes envolvendo vazamento de informações sigilosas são causados pelos próprios funcionários, o que vem demandando: (i) uma atenção cada vez maior por parte das empresas no sentido de treinar e conscientizar seus colaboradores acerca de questões ligadas à segurança da informação; e (ii) atuação mais enérgica no âmbito jurídico nos casos de desvio de informações, visando não só a minimizar os prejuízos e riscos causados por um caso especifico, mas também como forma de coibir novos casos em um processo educativo.

Nessa linha, é preciso ter em mente que, muito embora os funcionários tenham acesso às informações da empresa, não significa que estas pertençam a eles, de modo que os colaboradores devem redobrar os cuidados com os quais tratam os dados que passam por suas mãos, principalmente no que diz respeito ao envio ou armazenamento dessas informações, sob pena de responsabilização pessoal. Da mesma forma, as empresas deverão estar cada vez mais vigilantes com relação às ações tomadas com suas informações, sem, contudo, invadir a privacidade de seus funcionários.

Cabe aqui lembrar algumas recomendações de como as empresas deveriam se proteger em face do mau uso das informações por parte dos funcionários. O primeiro passo é, sem dúvida, implementar medidas de conscientização da inexistência de expectativa de privacidade que os funcionários possam ter ao utilizar dispositivos de uso corporativo. Essa "quebra de expectativa" pode ser feita mediante sucessivos avisos de monitoramento do ambiente virtual da companhia, campanhas de conscientização, bem como a previsão expressa da existência de controles no uso de ferramentas tecnológicas, de controles das atividades e da determinação de que os dispositivos eletrônicos da empresa deverão ser utilizados para fins estritamente profissionais.

Recomenda-se, ainda, que tais previsões que visam a legitimar o referido monitoramento estejam expressas em diversos documentos internos das empresas, tais como contratos de trabalho, código de condutas; regulamento interno de segurança da informação (RISI) e Termos de uso de sistemas de informação (TUSI), justamente para também dar validade a qualquer prova que for obtida por meio do monitoramento implementado.

Toda essa preocupação com a segurança das informações decorre do fato de que todos documentos e informações, além de terem uma alta importância mercadológica, constituem a chamada "propriedade imaterial" das empresas e, logo, podem ser utilizados única e exclusivamente por estas, o que é assegurado pela Constituição Federal em seu artigo 5º, incisos XXII e XXIX, bem como pelas Leis 9.279/96 (Lei de Propriedade Industrial) e 9.610/98 (Lei de Direitos Autorais), além de outras normativas específicas.

Com efeito, a partir do desvio indevido das informações e documentos, nasce para as empresas que tiveram seus direitos violados a prerrogativa de proceder à rescisão do contrato de trabalho por justa causa, dada a gravidade do ato cometido, o que inclusive corrobora a tese jurídica futura de que os atos cometidos são ilícitos e merecem reparação. Não obstante a dispensa por justa causa, também poderão ser propostas ações judiciais, no âmbito da Justiça do Trabalho, a fim de que os colaboradores se abstenham de utilizar as informações sigilosas, bem como as excluam de seus dispositivos (celulares, computadores, *tablets*, *pen drives* e etc), sem prejuízo da apuração de danos eventualmente sofridos, conforme permite o artigo 207 da Lei 9.279/96, gerando direito de indenização para as empresas pelos danos causados.

Atualmente, muito embora essa não seja uma matéria corriqueira na justiça laboral, já existem diversas decisões judiciais em todo o país condenando ex-funcionários de empresas em casos de vazamento de informações sigilosas, inclusive com multas de grandes montas em caso de uso, exploração ou divulgação dos dados. Nesse tocante, o Tribunal Superior do Trabalho, em recente decisão no âmbito do RO 101576-28.2016.5.01.0000, manteve a dispensa por justa causa de empregado bancário que enviou dados de clientes para seu e-mail pessoal, por entender que informações sigilosas ficaram expostas em

ambiente desprotegido, incidindo na hipótese prevista no artigo 482, alínea “h”, da CLT, que prevê a indisciplina e a insubordinação como motivos para a dispensa por justa causa.

Ainda a esse respeito, é importante destacar que a legislação vigente estipula que, salvo previsão expressa em contrário, pertencem ao empregador as criações industriais desenvolvidas por funcionário em virtude da execução do contrato de trabalho. A título exemplificativo, mencione-se os artigos 88 da Lei 9.279/96 e 4º da Lei 9.609/98.

Por fim, consigne-se que a redação do artigo 195, incisos XI e XII, da Lei 9.279/96 caracteriza como crime de concorrência desleal a divulgação, exploração ou utilização, sem autorização, de conhecimentos, informações ou dados confidenciais utilizáveis na indústria, comércio ou prestação de serviços, principalmente quando obtidos por meios ilícitos, sendo a hipótese, os casos de desvio de informações e/ou documentos sigilosos. A pena para esses casos é de 3 meses a 1 ano, ou multa.

Diante disso, temos que a segurança da informação constitui um tema de extrema sensibilidade para as empresas, justamente por ser o fator humano o maior risco à segurança das informações e o maior causador de incidentes, levando as empresas a, cada vez mais, investirem quantias significativas em softwares a fim de evitar o vazamento de informações privilegiadas e em ações judiciais pós-incidentes, visando a minimizar os prejuízos e coibir novos casos, e, assim, consequentemente, tornando-as menos vulneráveis de dentro para fora, mitigando, inclusive, riscos ligados às sanções previstas na Lei 13.709/2018 (Lei Geral de Proteção de Dados) em caso de incidentes de vazamento de dados pessoais.

[1] São exemplos de Shadow IT: utilização de Onedrive, Google Drive, Dropbox ou GitHub.

[2] Para saber mais, leia: https://www.rutter-net.com/blog/4-security-risks-of-shadow-it

[3] Disponível em https://www.kaspersky.com.br/about/press-releases/2017_em-40-das-empresas-do-mundo-todo-funcionarios-escondem-incidentes-de-seguranca-de-ti. Acesso em 12.11.2018.

Date Created
14/12/2018