O *home office* e a proteção dos dados pessoais

O surto mundial do novo Coronavírus (COVID-19) obrigou as empresas brasileiras a tomarem medidas extremas, e muitas vezes inesperadas, a fim de amenizar os riscos e proteger os seus colaboradores e clientes e, ainda, minimizar os eventuais prejuízos causados pela crise econômica.

Uma das medidas, se não primeira e mais comum, é a adoção da modalidade de trabalho *home office*, ou seja, trabalho remoto. Assim, os colaboradores podem exercer suas funções (ou, ao menos, a maioria delas) em casa, respeitando os protocolos de segurança para diminuir os riscos de contágio e propagação da doença, sem a necessidade de impactar demasiadamente a produtividade da empresa.

Em situações normais, o processo de adoção do *home office* levaria alguns dias (ou até meses), já que exige certo preparo tecnológico e implantação de diretrizes específicas de segurança da informação para tanto. Contudo, considerando a seriedade e emergência vividas há alguns dias, as empresas se viram obrigadas a implantar o sistema de forma rápida e inesperada, o que infelizmente pode trazer muitos problemas.

Pensando na proteção dos dados pessoais a que os trabalhadores têm acesso, que normalmente é realizado somente dentro da

empresa, a adoção do *home office* é delicada e requer uma série de cuidados, principalmente considerando o fato de que, muitas vezes, os computadores e *notebooks* pessoais são compartilhados com outras pessoas, que em nada se relacionam com a empresa.

E nem é preciso ir tão longe. Uma simples chamada telefônica, quando realizada em casa, pode dar azo à divulgação de informações confidenciais a terceiros não autorizados, mesmo que não intencionalmente.

A Lei Geral de Proteção de Dados (LGPD), que entra em vigor em agosto deste ano, surgiu para garantir e intensificar a proteção ao tratamento de dados. Ela é aplicável a qualquer pessoa (física ou jurídica), cujas atividades abranjam a utilização de dados pessoais. Desta forma, afeta todas as empresas, sejam elas de pequeno, médio ou grande porte.

Os dados pessoais a que a legislação se refere consistem em qualquer informação relativa a uma pessoa natural, identificada ou identificável. Ou seja, seu nome, endereço, RG e CPF, por exemplo.

Apesar de ainda não ter entrado em vigor, é de extrema importância que as empresas se preparem para a implantação de suas normas e, desde já, respeitem as suas diretrizes. E isso conta, inclusive, com a correta instrução e medidas adotadas para a modalidade de trabalho *home office*, principalmente neste momento em que há extrema urgência e rapidez na adoção da medida.

Para evitar o vazamento de dados e realizar o trabalho remoto de forma segura, tanto ao trabalhador quanto à empresa, algumas regras e orientações podem ser aplicadas. Por exemplo:

1. Bloqueio da tela do *notebook* ou computador após um período determinado sem uso, com a exigência de senha para voltar à ativa;

2. Providenciar e garantir uma conexão segura com a internet nos aparelhos pessoais;

3. Garantir que os aparelhos e equipamentos pessoais dos colaboradores sejam compatíveis com os sistemas utilizados pela empresa;

4. Instruir e treinar firmemente os colaboradores a manter a privacidade e sigilo das informações;

5. Possuir, ainda, regras quanto aos documentos físicos que podem ser levados para casa: quais são eles, quem poderá levar e qual a forma de controle sobre a entrada e saída destes documentos da empresa;

6. Usar proteção antivírus eficaz;

7. Possuir, para casos de extravio de dados, um plano de ação para minimizar o vazamento e a gravidade do ocorrido.

Assim, vê-se que, quando se fala em vazamento e proteção de dados pessoais, todo cuidado é pouco, e as empresas devem se preparar para seguir rigorosamente as medidas que serão, em um futuro bem próximo, impostas pela Legislação, a começar pela situação excepcional que o mundo todo está vivendo.

Artigo escrito pela advogada **Laís Silveira** que integra a equipe da área cível da **FCQ Advogados**