

Opinião: O controle dos colaboradores por meio da tecnologia

No último ano, diversas empresas foram obrigadas a se adequar à rotina de *home office*, criando meios de controlar a produtividade e a atuação de seus colaboradores. E, nesses casos, um tema já conhecido da Justiça Trabalhista ganha relevo: quais são os limites do "poder diretivo"? A expressão é utilizada para definir os direitos de controle que a empresa exerce sobre o funcionário, tais como monitoramento de e-mails, captura de telas de trabalho, câmeras e até mesmo a geolocalização de *smartphones*



E se você está se perguntando se as empresas podem fazer

isso, a resposta é clara: podem, sim. Contudo, esse Big Brother Brasil corporativo merece atenção e cuidado, uma vez que excedidos os limites constitucionais, essa coleta desenfreada de informações pode gerar transtornos tanto para a empresa quanto para o empregado.

No ano passado, finalmente, entrou em vigor a Lei Geral de Proteção de Dados (LGPD), que dispõe sobre coleta, tratamento e armazenamento de dados pessoais em todo o país e, mesmo que as sanções administrativas passem a valer somente em agosto próximo, existe a possibilidade de responsabilizar civilmente as empresas por vazamentos e danos de ordem material e moral que ocorram em razão da coleta de informações. Assim, as empresas que lidam com dados sensíveis do colaborador, tais como a biometria, informações de saúde, entre outros temas que possam gerar discriminação, devem registrar o consentimento do titular e deixar claro os motivos para a coleta, a forma de armazenagem e o meio de uso.



Nesse sentido, o monitoramento irrestrito dos colaboradores poderá ensejar a coleta de dados desnecessários ou, pior ainda, que nem sequer pertençam ao colaborador. Vejamos a seguinte hipótese: o funcionário João configurou em seu apartamento um espaço para o desempenho de suas funções de *home office*, dispondo de *notebook* e *smartphone* da empresa. Contudo, para que seja possível o seu monitoramento empresarial, deve utilizar um *software* de reuniões *online* constantemente conectado durante o expediente, de modo que a câmera do *notebook* capture imagem e áudio de seu ambiente de trabalho. Maria, esposa de João, também em *home office*, utiliza o mesmo ambiente da casa para trabalhar e exerce a função de atendimento ao consumidor numa empresa de *call center*. Diariamente, Maria recebe ligações de clientes e coleta seus respectivos dados, sensíveis ou não, para que possa consolidar o atendimento; tudo isso enquanto a câmera de João registra som e imagens do ambiente.

No cenário narrado, apesar de João dar seu expresso consentimento para a captura de suas informações pelo empregador, Maria não o fez e mesmo assim tem sua imagem (dado sensível) coletada, bem como o áudio no qual trata de assuntos do trabalho e, entre eles, informações dos clientes da empresa contratante. Nesse momento, a importância de adequação à lei grita alto. Em que pese a lei jamais impedir a coleta dos dados, ela regulamenta o tratamento daquelas informações que não forem estritamente necessárias para quem as coleta; nesse caso, não resta dúvida, devem ser descartados.

Sim, os dados coletados, seja por meio de imagens, e-mails ou documentos, após o devido tratamento por quem os coletou, devem ser eliminados das bases de dados ou mecanismos de armazenamento da empresa (*backups* e servidores). Ou seja, alcançada a finalidade da coleta proposta ou terminado o período necessário de armazenamento, a LGPD determina expressamente que os dados coletados devem ser eliminados.

Outra tarefa da empresa é a orientação didática. A cultura da proteção de dados deve ser disseminada desde a entrada do colaborador, por meio de políticas internas da corporação. A implementação de sistemas efetivos de proteção de informações está inteiramente ligada à cultura interna da empresa, evitando-se, em última análise, multas e condenações.

Mas não cabe somente à empresa proteger os dados do colaborador: a pessoa física também é responsável pela utilização das tecnologias voltadas à diminuição dos incidentes. Misturar vida pessoal e profissional nos dispositivos da empresa pode ser perigoso; importante lembrar que não é possível "desfazer" o que já foi compartilhado.

Utilizar o computador da empresa, ou mesmo um *smartphone*, pode ser um facilitador para a imensa maioria das pessoas, contudo, a atenção deve ser redobrada. Utilizá-los para acessar sites, conversas particulares e armazenamento de arquivos pessoais pode ser prejudicial. Além disso, armazenar senhas pessoais, encaminhar *e-mails* impróprios e instalar softwares pode complicar a vida do colaborador. Sugerimos alguns cuidados para se tomar a partir de agora:



Não conecte o equipamento de trabalho a redes públicas

A facilidade para trabalhar em qualquer lugar pode ser sedutora, mas o uso de *coworkings* ou cafés para trabalho representa perigo. É comum estabelecimentos disponibilizarem Wi-Fi aos clientes por meio de um simples cadastro. Se a sua ocupação profissional pressupõe o tratamento de dados sensíveis ou informações confidenciais, conectar seus dispositivos a redes sem fio abertas permite o acesso de terceiros mal-intencionados. Criminosos podem criar pontos de Wi-Fi falsos para roubar dados de quem os utiliza e, a partir da criação de um *login*, rastrear sites, documentos e senhas utilizados. E mesmo que não ocorra algo criminoso, a mera troca de dados pelo acesso pode causar incômodos ao usuário, que pode ter seus dados comercializados e a partir daí, sofrer o desagradável bombardeio dos *e-mails marketing*.

Não acesse sites de vagas usando o e-mail da empresa

Que o mundo corporativo está em constante mudança, todos sabemos. Ocorre que acessar sites de vagas prejudica a imagem do funcionário porque não é ético enviar currículos pelo e-mail corporativo. Além de as empresas possuírem acesso aos e-mails trocados e sites navegados, também podem monitorar o salvamento de documentos com palavras chaves como "currículo.doc".

Não acesse sites impróprios ou instale softwares não permitidos

Empresas costumam adotar políticas rígidas na área de TI, seja pelo bloqueio de acesso a sites ou instalação de programas. Isso se dá porque diversos sites impróprios estão repletos de vírus e *malwares* que podem roubar informações dos computadores. Assim, o objetivo principal dessas proibições é evitar contração de vírus ou uso de *softwares* ilegais. Cabe lembrar que navegar em páginas impróprias pode configurar motivo suficiente para demissão por justa causa.

Cuidado com armazenamento remoto

Armazenar documentos em nuvem merece redobrada atenção. A possibilidade de acessá-los em qualquer lugar não pode ser atrativo para armazenar documentos pessoais. Uma vez incluídos na nuvem, a empresa tem pleno acesso.

Tal qual o casamento, não há fórmula mágica. Mas isso não significa que nada deva ser feito, já que a inércia é a pior opção. No final do dia, a lição de casa para as empresas é o desenvolvimento de ações junto aos colaboradores, com participação das áreas de TI, recursos humanos e jurídico. O segredo do sucesso está na via de mão dupla, na qual a empresa atua de maneira a proteger informações e garantir um ambiente digital seguro, cabendo aos funcionários a adoção de boas práticas, respeitando as diretrizes da corporação e prezando pelo interesse dos clientes.

Date Created

24/05/2021