

## O Desafio da Proteção de Dados Pessoais nas Relações de Trabalho

O tema da proteção de dados vem, nos últimos anos, se tornando mais robusto e importante, com a entrada em vigor de leis que tratam da matéria.

O início de toda a discussão ocorreu com a promulgação da Lei 12.965/2014, mais conhecida como “Marco Civil da Internet”, que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.

Em complemento, foi promulgada a Lei 13.709/2018, que dispõe, exclusivamente, sobre a proteção de dados pessoais e que foi alterada pela Medida Provisória 869, de 27 de dezembro de 2018, que, inclusive, estabeleceu um prazo de 24 (vinte e quatro) meses para a entrada em vigor das disposições da Lei 13.709/2018.

Nesse sentido, as empresas têm até agosto/2020 para se organizarem e criarem mecanismos para a proteção dos dados pessoais de clientes, fornecedores, empregados, prestadores de serviço, etc.

Especificamente, no âmbito das relações de trabalho, é fundamental que as empresas passem a tratar, de forma bastante cuidadosa, os dados pessoais dos candidatos, empregados e prestadores de serviço, para evitar a aplicação das pesadas multas previstas na legislação, que podem chegar a 2% do faturamento da empresa, grupo ou conglomerado no Brasil em seu último exercício fiscal, limitadas à surpreendente monta de R\$ 50 milhões.

Ou seja, o valor arbitrado à multa por descumprimento da Lei Geral de Proteção de Dados já evidencia a importância do assunto na atualidade e a dimensão do cuidado que as empresas devem ter com as informações pessoais que lhes são disponibilizadas.

Em linhas gerais, a lei define como dados pessoais, quaisquer informações relacionadas à pessoa natural identificada ou identificável (nome, domicílio, telefone, CPF, etc.) e dados sensíveis como qualquer dado pessoal passível de maior potencial discriminatório em relação ao seu titular (origem racial ou étnica, convicção religiosa, condição médica, opinião política, filiação a sindicato, orientação sexual, etc.).

Dessa maneira, desde o primeiro contato com um candidato a uma vaga de emprego, a empresa deve tratar, com responsabilidade, as informações pessoais recebidas, sendo imperioso solicitar apenas os dados essenciais a uma finalidade específica e adequação determinada, sem excessos, para evitar futuras alegações de discriminação na contratação, por exemplo.

Para tanto, um exemplo de medida que visa à proteção da empresa contra esse tipo de alegação seria a adoção de formulários claros que evidenciem a livre e inequívoca manifestação do candidato, por meio da qual ele concorda com o tratamento de seus dados pessoais para a específica e exclusiva finalidade de concluir o processo seletivo e viabilizar o registro e o cumprimento das demais obrigações acessórias trabalhistas, caso concretizada a contratação.

Da mesma forma, vislumbramos a necessidade de inclusão de cláusulas específicas nos contratos de trabalho, com relação ao tratamento dos dados pessoais dos empregados e de seus familiares, para fins, por exemplo, de inclusão das pessoas no plano de saúde, seguro de vida, plano odontológico e afins.

Nesse passo, imprescindível, ainda, a revisão dos contratos de prestação de serviços firmados com terceiros que terão acesso e, por consequência, manipularão tais dados, tais como operadoras de planos

de saúde, seguro de vida e empresas de gestão de folha de pagamento, sendo recomendável a inclusão de cláusulas expressas sobre a forma de tratamento e proteção dos dados transferidos, bem como a responsabilidade em caso de eventual vazamento.

Outro ponto bastante sensível diz respeito às informações relacionadas à saúde dos trabalhadores que, apesar de já protegidas pelo sigilo médico, merecem especial atenção quanto ao armazenamento e divulgação de atestados e exames médicos, compra de medicamentos por meio de convênios e utilização de plano de saúde, a fim de preservar a intimidade do empregado e seus familiares.

Aqui é importante lembrar o quanto disposto na Resolução nº 1819/2007, do Conselho Federal de Medicina, que proíbe a inclusão da CID (Classificação Internacional de Doenças) nos atestados médicos, em casos específicos, sem a expressa autorização do paciente, justamente para proteger sua intimidade.

Com isso, em termos práticos, as empresas deverão rever suas políticas internas, definindo, de forma bastante clara, os setores que poderão ter acesso aos dados de candidatos, empregados e terceiros, bem como a forma de utilização de tais informações, mapeando e identificando potenciais falhas em *compliance*, sendo, ainda, responsáveis pela orientação e treinamento do pessoal que manipulará os dados.

Outro aspecto bastante relevante diz respeito ao fato de que empresas multinacionais, em geral, precisam compartilhar esses dados com a matriz situada no exterior. Torna-se imprescindível obter o consentimento do titular da informação, caso essa transferência de dados não ocorra em decorrência de uma obrigação legal, mas apenas para fins de manutenção/atualização de banco de dados, bem como contar com um sistema que garanta a máxima proteção dessas informações no processo de compartilhamento.

Como se vê, a melhor forma de tratar esse assunto é com bastante transparência e conscientização, no sentido de que as informações pessoais devem ser coletadas e utilizadas apenas para os fins legais e específicos, sem qualquer desvirtuamento de finalidade.