Por Camila Camargo e Marco Zorzi (*)

No cenário atual de pandemia, no momento de retomar as atividades presenciais, as empresas são recomendadas a adotar, além de medidas de distanciamento social que não envolvam o tratamento de dados pessoais (por exemplo, mediante a utilização de aplicativos que contam o número de pessoas que entram e saem de um determinado lugar), protocolos específicos para o ingresso e acesso ao ambiente de trabalho, a fim de identificar pessoas com possíveis sintomas da doença.

Nessa última categoria, as medidas mais frequentes incluem a medição de temperatura, questionários a serem respondidos para possibilitar a entrada tanto na empresa como nas dependências de clientes, fornecedores e parceiros de negócios (por exemplo, em procedimentos de integração para prestação de serviços no local) e até mesmo a utilização de aplicativos para realização desse controle.

Considerando que as operações de acesso, coleta e consulta de dados pessoais estão incluídas na definição de “tratamento de dados pessoais” do art. 5º, X, da Lei Geral de Proteção de Dados (LGPD), vigente desde 18 de setembro de 2020, as empresas que realizarem coleta, armazenamento e/ou manuseio de dados pessoais de seus próprios colaboradores e de terceiros deverão ser cautelosas na realização de tais atividades.

Ademais, é fundamental lembrar que o objetivo de redução de riscos de contágio de covid-19 é manter colaboradores, clientes, prestadores de serviços e visitantes que ingressam nas dependências das empresas seguros e não as exime, em nenhuma hipótese, das obrigações intrínsecas ao tratamento dos dados pessoais, além das demais regras de direito do trabalho aplicáveis.

Dito isso, como cuidar desses dados pessoais de saúde (sensíveis) de forma correta e adequada?

Apresentamos abaixo algumas dicas práticas, elaboradas a partir de princípios da LGPD:

1. **Seja transparente**: é preciso que fique muito claro como a empresa vai tratar dados pessoais triviais e dados pessoais sensíveis, incluindo informações sobre como serão descartados de forma segura quando não forem mais necessários, assim como a garantia de que serão utilizados apenas pelo tempo necessário para esse controle. Essas informações devem ser em regra disponibilizadas antes da coleta dos dados pessoais e publicadas em documentos de fácil acesso pelo titular de dados (colaboradores da própria empresa ou de terceiros). Neste sentido, ganham destaque a política de privacidade publicada no site da empresa (para terceiros), bem como os avisos de privacidade para colaboradores. Tais documentos devem ser atualizados ou criados para refletir de forma transparente o tratamento de dados pessoais no caso concreto, devidamente legitimados conforme as bases legais previstas especialmente no art. 11 da LGPD.
2. **Adote medidas técnicas de segurança**: manter os dados pessoais em ambiente seguro, por meio de medidas que garantam a integridade, disponibilidade e confidencialidade são medidas de caráter preventivo sempre recomendadas. Na prática, um incidente de segurança pode causar o vazamento dos dados pessoais e, potencialmente, prejuízos para a empresa (regulatórios e reputacionais), violando, consequentemente, os direitos daqueles que tiveram seus dados pessoais expostos. Assim sendo, é relevante revisar as formas de armazenamento de dados pessoais e assegurar que eventuais parceiros que estejam tratando esses dados (por exemplo, fornecedores de aplicativos) tenham também medidas técnicas de segurança aptas a proteger os dados pessoais.
3. **Use apenas o que é preciso para cumprir o objetivo**: este ponto merece atenção especial, à luz da variedade de formas aplicadas pelas empresas para coletar os dados pessoais, em virtude dos protocolos de segurança durante a pandemia. Em qualquer caso,

apenas os dados necessários, adequados e relevantes devem ser coletados. Note que um dado pessoal pode ser útil, mas não necessário. Por exemplo: se a finalidade de medir a temperatura é verificar se, no momento do ingresso, a pessoa não tinha temperatura acima do normal; uma vez que tal verificação é realizada, a finalidade encerra-se e, dadas algumas exceções, a informação pode ser descartada. Ou ainda, quando são exigidos exames de terceiros que visitarão a empresa, é recomendado avaliar se há finalidade posterior para o armazenamento dos respectivos resultados ou se é possível descartá-los. Da mesma forma, em caso de resultados positivos, recomenda-se abster-se de solicitar informações adicionais como os locais específicos visitados ou outros detalhes relacionados à esfera privada do indivíduo.

Finalmente, para reduzir o acesso aos dados de saúde coletados, é preferível que as operações de tratamento dos dados pessoais sejam realizadas por um grupo restrito de indivíduos. Caso a empresa disponha de um médico interno, esta figura oferece uma garantia importante, também em virtude do vínculo de sigilo profissional. Vale lembrar que, caso a sede da empresa esteja localizada em um prédio, condomínio ou centro de negócios que adota seus próprios protocolos de ingresso, medidas (inclusive contratuais) deverão ser adotadas para garantir que os dados dos colaboradores e parceiros de negócios sejam tratados conforme as normas aplicáveis.

(*) **Camila Camargo** é advogada do Departamento Societário da Andersen Ballão Advocacia, responsável por proteção de dados e propriedade intelectual.

(*) **Marco Zorzi** é consultor de proteção de dados da Andersen Ballão Advocacia.