Por Wilson De Faria e Camilla Chizzotti (*)

A Lei Geral de Proteção de Dados Pessoais (“LGPD”), como claramente determina seu texto, regulamenta o “tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade”. Em que pese a proximidade da sua entrada em vigor, há uma movimentação ainda tímida das organizações de saúde em busca de adequação. Essa timidez decorre em grande parte do desconhecimento acerca da abrangência da norma, do seu enforcement e da sua aplicabilidade.

Uma parcela dessas instituições pode estar ainda presa à cultura do “quanto mais dados, melhor” e ter receio de que a adequação à LGPD venha a engessar processos internos e principalmente dificultar o processamento ou a prospecção de serviços de saúde. Isso não é necessariamente verdadeiro.

O primeiro passo para adequação à norma é a realização de um mapeamento de dados para que haja clareza de quais dados são tratados e a forma/processo como isso é realizado no contexto da rotina interna. Esse mapeamento possibilitará revisitar processos e procedimentos internos de maneira a simplificá-los e otimizá-los, gerando economia de tempo e recursos, além de evitar riscos existentes ao tratar dados desnecessários e em excesso.

A complexidade da implementação de um programa de privacidade e proteção de dados dependerá diretamente da maturidade dos processos e procedimentos já existentes na empresa, da quantidade e forma em que ocorrem os fluxos de tratamentos de dados pessoais e do comprometimento da alta direção em engajar os demais colaboradores em um processo de aculturamento geral acerca da nova governança atrelada a privacidade, segurança e gerenciamento de dados pessoais.

Após o mapeamento inicial é necessária a criação de uma Política de Privacidade de Dados clara e objetiva contendo todos os pilares da governança a ser instituída, além de diretrizes como procedimentos internos, plano de resposta a incidentes, avaliação de riscos de novos projetos ou produtos (privacy by design), tipos de dados tratados e suas finalidades, riscos envolvidos no tratamento de dados, compartilhamento com terceiros e transferências internacionais, indicação e informações de contato do Encarregado (Data Processing Officer - DPO), direitos dos titulares e formas de garanti-los, entre outros temas que a instituição julgar relevantes.

Cumpre ressaltar que cada setor e ramo de atividade terão demandas específicas para adequação à norma. Clínicas, instituições de saúde e hospitais, pela própria natureza de sua atuação, lidam diariamente com dados pessoais sensíveis, que trazem maiores riscos se vazados e demandam cuidados adicionais e específicos.

Vale mencionar que na relação paciente-hospital ou paciente-clínica, a instituição de saúde desempenha o papel de controlador de dados, o que lhe atribui maior conjunto de deveres e atribuições para estar em conformidade e riscos mais elevados de responsabilização ou possibilidade de penalização pela não adequação.

As atividades dos profissionais de saúde são regidas por normas setoriais que já fazem referência a alguns tipos de tratamentos de dados pessoais. Assim, a adequação à LGPD deverá ser feita através da interpretação conjunta de todas as normas pertinentes, como a lei que dispõe acerca das medidas relacionadas ao prontuário do paciente (Lei nº 13.787/18) e o Código de Ética Médica do Conselho Federal de Medicina.

Tomemos como exemplo a Lei nº 13.787/18, que regulamenta a forma de digitalização, guarda e manuseio do prontuário médico. Sob um olhar rápido, que não leve em consideração os preceitos da LGPD, pode parecer que a lei do prontuário do paciente é suficiente para regulamentar o tratamento dos dados aos quais o documento faz referência. Porém, sob o ponto de vista de adequação à LGPD, a adequação apenas à lei do prontuário é insuficiente.

Isso porque a elaboração de um prontuário médico é precedida por diversos tipos de tratamentos

de dados pessoais, como coleta, processamento, guarda em sistemas internos das instituições, compartilhamento com laboratórios e planos de saúde, dentro outros, e nenhum desses tratamentos é regulamentado pela Lei nº 13.787/18.

Lembremos que o custo da não implantação de um programa de privacidade e proteção de dados pode ser a sobrevivência da própria empresa, pois além das pesadas multas por infração e multas diárias que podem variar (cada uma delas) de 2% do faturamento da empresa a R$ 50 milhões, outras sanções como a publicização da infração, suspensão, bloqueio do tratamento de dados e até mesmo a condenação à exclusão dos dados pessoais dos repositórios da empresa. Essa medida extrema pode afetar imensamente o funcionamento da instituição de saúde pois pode levar à paralização das atividades que necessitem do tratamento dos dados pessoais.

Ademais, a ocorrência de um incidente de segurança e sua publicização na mídia acarretará um dano reputacional por vezes irreparáveis às instituições.

Há hoje uma convergência internacional sobre o direito fundamental à privacidade informacional. Empresas de capital internacional atualmente já buscam parceiros de negócios ou fornecedores com nível de proteção de dados adequado. As empresas em conformidade certamente perceberão um incremento em sua capacidade concorrencial, além do ganho reputacional perante os titulares de dados. As instituições de saúde não serão diferentes.

(*) **Wilson De Faria** é sócio sênior da WFaria Advogados. Formado em Direito pela USP, em Administração de Empresas pela FGV-SP, com pós-graduação no CEU – São Paulo, INSEAD- França (MBA) e Harvard Business School – USA (OPM).

(*) **Camilla Chizzotti** é advogada sênior da WFaria Advogados. Graduada em Direito pela Pontifícia Universidade Católica de São Paulo. Pós-graduada na London School of Business.