

Por Paula Viana (*)

Que a nova era digital trouxe avanços e benefícios à sociedade é incontestante. Não obstante, é fato que o preço a se pagar está diretamente relacionado ao abalo de direitos como a privacidade, o sigilo e a dignidade. E um dos setores que sofrerá impacto direto das inovações é o da saúde.

Influenciado pela GRPD (General Data Protection Resolution) europeia, o Brasil publicou a nova Lei Geral de Proteção de Dados (Lei 13.709/2018), que representa uma inovação na regulamentação do tema no país, na esteira do Marco Civil da Internet. Em seu artigo 5º, define como dado pessoa sensível aquele referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural, o que significa que somente poderá ser tratado em algumas hipóteses elencadas em lei, tal como a tutela da saúde.

As instituições e profissionais da saúde deverão realizar adequações estruturais e comportamentais para que se alcance a segurança dos dados. Deverão repensar todos os seus processos de coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração de dados dos pacientes.

Há, portanto, muito a fazer. Desde a entrada do paciente e preenchimento da ficha cadastral até as informações registradas em prontuário, passando por fornecedores, prestadores de serviço, colaboradores e laboratórios. Todos precisarão ser preparados para a nova realidade, uma vez que a penalidade prevista é alta, além do evidente desgaste pelo qual passaria uma instituição de saúde diante de uma notícia de vazamento. O prazo para que essas adaptações sejam programadas e efetivas é agosto de 2020.

A mídia, com uma frequência alarmante, tem publicado casos envolvendo vazamento de dados, inclusive no setor de saúde, no Brasil e no mundo.

OS EUA, desde 1996, apresentam legislação sobre privacidade de dados (HIPAA – a Lei de Portabilidade e Responsabilidade de Seguro Saúde), com o objetivo de proteger registros médicos e outras informações de saúde. Ainda que já esteja há mais de 20 anos à frente do Brasil no quesito da regulamentação, vazamentos ocorreram nos EUA e as empresas estão gastando fortunas com multas e investimentos em segurança dos dados. Por exemplo, a Anthem foi multada em US\$ 16 milhões e precisou pagar ainda US\$ 115 milhões em um acordo para encerrar uma ação coletiva proposta por aqueles que tiveram seus dados violados.

Informações de saúde despertam muito interesse de hackers. Afinal, paga-se muito bem no mercado, porque com base em perfis de pacientes, grandes empresas poderão adaptar ou criar produtos com mercado consumidor garantido. De outro lado, seu compartilhamento, dentro dos limites da legalidade, fornece subsídios para uma melhoria das ações de saúde pública, a investigação clínica e epidemiológica.

A lei determina que todas as informações precisarão estar em ambientes controlados e comprovadamente seguros. Além disso, também é de suma importância implantar soluções, para tanto as instituições deverão adotar redes criptografadas, softwares de monitoramento, mas especialmente preparar as pessoas que terão acesso aos dados – por mais sofisticado que seja um sistema de proteção, será o ser humano o responsabilizado por qualquer vazamento.

A Medida Provisória de 869/2018, publicada para aprimorar a Lei 13.709/18, criou a Autoridade Nacional de Proteção de Dados, responsável pela regulamentação de procedimentos previstos na lei. Não obstante, mal foi publicada e já conta com nada menos que 176 emendas parlamentares a serem analisadas. A ANPD é de suma importância para que a lei possa ser efetiva.

Algumas dessas emendas tratam diretamente do tema saúde. Como exemplo, a Emenda 121 que

versa sobre autorização para a troca de dados sensíveis de saúde para comunicação entre prestadores de serviços. Já a emenda 120 pretende a inclusão de entidades com fins lucrativos como órgão de pesquisa e que, portanto, passariam a poder tratar dados pessoais (na redação atual apenas órgãos de pesquisa sem fins lucrativos preenchem o requisito disposto no art.7º, inciso IV).

Um dos maiores desafios será o controle dos dados pessoais. A Lei 13.709 dispõe que o tratamento dos dados pessoais deverá observar a finalidade, a qual deverá ser apresentada ao titular de forma explícita, sem que haja a possibilidade de os dados serem tratados para outro fim. A penalidade para o descumprimento da legislação é significativa: multa simples, de até 2% do faturamento da pessoa jurídica de direito privado alcançando até R\$ 50 milhões por infração. No entanto, o prejuízo maior está em tornar pública a infração, haja vista que a instituição perderá sua credibilidade por não cuidar dos dados de seus clientes/pacientes.

A legislação, ainda que careça de regulamentação em vários aspectos, representa um avanço. A partir da criação de um órgão específico para zelar pela proteção dos dados pessoais, a fiscalização poderá coibir os abusos, determinar medidas técnicas de segurança a serem adotadas pelas instituições e punir, administrativamente, o mau uso de dados.

Resta aos cidadãos esperar o cumprimento da lei.

(*) **Sandra Franco** é consultora jurídica especializada em direito médico e da saúde, doutoranda em saúde pública, ex-presidente da Comissão de Direito Médico e da Saúde da OAB de São José dos Campos (SP), presidente da Academia Brasileira de Direito Médico e da Saúde e membro do Comitê de ética e Pesquisa em Seres Humanos da UNESP/SJC.

Fonte: [O Estado de S. Paulo](#), em 28.04.2019.