REFLEXOS DA LEI DE PROTEÇÃO DE DADOS NO ÂMBITO MÉDICO HOSPITALAR

Mayara Roth Isfer[1]

Com a promulgação da Lei Geral de Proteção de Dados Pessoais (Lei n.º 13.709/2018), em agosto de 2018, a necessidade de adequação do manejo de dados por empresas, entidades do terceiro setor, órgãos governamentais ou mesmo pessoas naturais passou a ser pauta permanente. Agora, restando menos de um ano para que as principais regras efetivamente entrem em vigor[2] – tornando cogentes as disposições previstas – a necessidade de alteração dos sistemas internos, de modo a respeitar a nova disciplina ganha cada vez mais urgência.

Embasada nos direitos à privacidade, à autodeterminação informativa, à liberdade de expressão, de informação, de comunicação e de opinião, à inviolabilidade da intimidade, da honra e da imagem, dentre outros direitos fundamentais, a Lei Geral de Proteção de Dados Pessoais (LGPD) criou uma regulamentação para o tratamento de dados pessoais no Brasil[3], nos âmbitos privado e público, estabelecendo quem são as figuras envolvidas e quais são os direitos e deveres decorrentes e as penalidades no caso de descumprimento – que podem chegar a R$ 50.000.000,00 (cinquenta milhões de reais) por infração (art. 52, II, da LGPD).

---

[1] A autora advoga na área de Direito Societário e Recuperacional no escritório Advocacia Felippe e Isfer, é mestre em Direito Comercial pela USP, graduada em Direito pela UFPR e graduanda no curso de Ciências Contábeis da Fipecafi.

[2] "*Art. 65. Esta Lei entra em vigor: I - dia 28 de dezembro de 2018, quanto aos arts. 55-A, 55-B, 55-C, 55-D, 55-E, 55-F, 55-G, 55-H, 55-I, 55-J, 55-K, 55-L, 58-A e 58-B; e II - 24 (vinte e quatro) meses após a data de sua publicação, quanto aos demais artigos.*"

[3] No que se refere ao âmbito de aplicação da Lei, o artigo 3º prevê que ela é utilizada em "*qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que: I - a operação de tratamento seja realizada no território nacional; II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou III - os dados pessoais objeto do tratamento tenham sido coletados no território nacional.*".

Para fins de compreensão da legislação, é essencial conceituar os principais sujeitos que permeiam as relações jurídicas legalmente abordadas. O primeiro deles é o próprio titular dos dados, isto é, a pessoa natural a quem se referem os dados pessoais que são objeto de tratamento. O controlador, por sua vez, é aquele a quem competem as decisões referentes ao tratamento de dados, enquanto que o operador seria o sujeito que realiza o tratamento dos dados em nome do controlador. O encarregado, finalmente, é o indicado pelo controlador e pelo operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados[4].

Com a entrada em vigor da Lei, as entidades deverão passar a indicar os responsáveis pelas supracitadas funções, cabendo a cada qual os deveres e responsabilidades previstos. O titular, por exemplo, terá direito de acesso às informações sobre o tratamento de seus dados, dentre as quais a identificação e as informações de contato do controlador, responsabilidades dos agentes que realizarão o tratamento (operador), finalidade do tratamento, etc.. Ademais, caberá ao controlador ou ao operador reparar os danos causados em razão das atividades de tratamento de dados e da omissão quanto à adoção das medidas de segurança previstas pela LGPD. Vê-se, assim, que a delimitação do âmbito de atuação de cada agente é essencial e deverá ser feita internamente pelas entidades.

Por outro lado, é possível dizer que a base da Lei de Proteção de Dados é o consentimento. Nessa linha, de um modo geral, é necessária a anuência do titular dos dados para que estes sejam tratados. A Lei prevê, todavia, outras hipóteses que dispensariam o consentimento; seriam elas: cumprimento de obrigação legal ou regulatória pelo controlador; no caso de administração pública, para tratamento e uso compartilhado de dados necessários à execução de políticas públicas; realização de estudos por órgão de pesquisa, priorizada a anonimização; quando necessário à execução de contratos ou de procedimentos preliminares à contratação; exercício regular de direitos em

[4] Criada pela Lei n.º 13.853/2019.

processos; proteção da vida ou da incolumidade física; tutela da saúde; quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalência dos direitos e liberdades fundamentais do titular que exija a proteção dos dados; e proteção do crédito.

No que se refere ao consentimento – permissivo mais comum para o tratamento de dados – este deve ser feito por escrito ou por outro meio que ateste a manifestação de vontade do titular. A cláusula que preveja o consentimento deve estar destacada e necessita conter a finalidade específica do tratamento, sob pena de nulidade. Deve igualmente haver consentimento expresso para a comunicação ou para o compartilhamento dos dados com outros controladores.

No caso de tratamento de dados autorizado pelo *legítimo interesse do controlador*, este deve estar baseado em finalidades legítimas, como o apoio e a promoção de atividades do controlador ou a sua proteção em relação ao titular. Nesses casos, apenas os dados necessários à finalidade pretendida poderão ser tratados. Ademais, a Autoridade Nacional de Proteção de Dados "*poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais*".

Partindo para os dados tratados em si, a LGPD separa-os em três categorias: (a) dado pessoal, considerado informação relacionada a pessoa natural identificada ou identificável, como nome, endereço, telefone, CPF, etc.; (b) dado pessoal sensível, compreendido como "*dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural*"; (c) dado pessoal de criança e de adolescente.

No que se refere aos dados pessoais sensíveis, seu tratamento depende de requisitos mais restritos, sendo autorizado em hipótese de consentimento expresso, cumprimento de obrigação legal ou regulatória, execução de políticas públicas, estudos por órgão de pesquisa, exercício regular de direitos, proteção da vida, da incolumidade física, da saúde e para a garantia da prevenção à

fraude e à segurança do titular. São aqui excluídas, portanto, as chamadas válvulas de escape da Lei (previstas nos incisos IX e X, e no §4º, do artigo 7º).

No âmbito médico hospitalar, apesar dos deveres de sigilo já existentes, as mudanças também serão sentidas. É que os hospitais, os centros médicos e as clínicas espalhadas pelo País tratam milhões de dados pessoais diariamente.

Hoje, para ser atendido na maioria absoluta dos estabelecimentos, o paciente deverá informar todos os seus dados básicos, como nome, endereço, RG, CPF, dados do plano de saúde, etc.. Ainda, para realizar exames e procedimentos, precisa informar os medicamentos que usa, suas doenças pré-existentes, condição atual de saúde, dentre outros. E, naturalmente, todos esses dados são armazenados. Após as consultas, são igualmente registrados internamente os prontuários médicos. O fluxo de dados tratados é, pois, enorme.

O Conselho Federal de Medicina já previa a necessidade de sigilo dos referidos dados no Código de Ética Médica de 2009. Todavia, atualizando as previsões anteriores, foi publicado em 1º de novembro de 2018 o novo Código de Ética Médica (Resolução CFM n.º 2.217/2018), mantendo intacta a proteção do sigilo do paciente e de seu prontuário.

Referida Resolução deve ser interpretada juntamente com Lei do Prontuário Eletrônico (Lei n.º 13.787/2018) e com a própria LGPD. Segundo a Lei do Prontuário Eletrônico, a digitalização dos documentos que compõem o prontuário é permitida, podendo-se descartar o original, desde que: (a) os métodos de digitalização reproduzam todas as informações contidas nos documentos originais; (b) no processo de digitalização seja utilizado certificado digital emitido no âmbito da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) ou outro padrão legalmente aceito; (c) o processo de digitalização obedeça a requisitos dispostos em regulamentos. Ainda, o artigo 4º da Lei prevê que "*os meios de armazenamento de documentos digitais deverão protegê-los do acesso, do uso, da alteração, da reprodução e da destruição não autorizados*".

Vê-se, assim, que no ambiente da saúde a LGPD foi acompanhada por outros diplomas igualmente voltados à proteção dos dados dos usuários. Nessa linha, buscando compatibilizar a realidade atual às novas regras que entraram e que entrarão em vigor, alguns passos são necessários, prevenindo as instituições de saúde em relação a possíveis sanções por vazamento de dados.

Primeiramente, considerando a necessidade de proteção dos dados dos titulares contra invasões externas e internas, é essencial o investimento em ferramentas para a segurança da informação, como antivírus, firewall, sistemas de detecção e de prevenção de invasão, etc.. A implantação de soluções de proteção e de segurança, com redes criptografadas e softwares de monitoramento é de suma importância, incluindo cláusulas com os prestadores de serviço respectivos acerca da responsabilidade pelo vazamento de dados.

Em um segundo momento, é imprescindível a reorganização interna dos dados e dos tipos de tratamentos destes, com sistemas diferentes para tipos de dados diversos, alteração das formas de restrição de acesso, mudanças de login, exclusão de acesso a ex-funcionários, etc.. A categorização e o monitoramento constante de todos esses dados é absolutamente essencial. Na mesma linha, a revisão de regras de privacidade e de políticas internas é igualmente importante, resultando em um sistema confiável.

Finalmente, considerando as novas regras relativas ao consentimento, é indispensável a alteração do sistema relativamente à concordância do titular, que deve contar com previsão clara e destacada acerca dos dados que serão tratados e da finalidade do tratamento, dentre outros aqui já comentados.

A observância dessas orientações possibilitará ao estabelecimento médico migrar com um mínimo de segurança para essa nova realidade relativa à proteção de dados.