Por Guilherme Ferri e Ricardo Medina (*)

A partir de agosto de 2020, empresas de todos os portes e segmentos precisarão garantir que seus stakeholders autorizem de maneira formal a coleta de suas informações pessoais. As companhias também devem garantir ao cliente o direito de saber a finalidade do mapeamento, quem terá acesso aos dados, como eles serão armazenados e se haverá compartilhamento das informações. A exigência passa a vigorar em virtude da nova Lei Geral de Proteção de Dados, também conhecida pela sigla LGPD.

Também é importante destacar que a Lei Geral de Proteção de Dados se baseia em 10 princípios:

1 - **Finalidade** – Dados coletados só podem ser tratados para fins legítimos e especificados aos titulares, ou seja, as empresas não podem coletar informações e, depois, usá-las para outros fins. Por exemplo, o hospital diz que vai utilizar um dado para fins de internação do paciente e depois utiliza a informação para compor uma pesquisa que será divulgada na imprensa.

2 - **Adequação** – O tratamento dos dados deve ser compatível com a finalidade que foi informada para o usuário. Ou seja, a empresa não pode usar os dados dos clientes para qualquer fim que não tenha sido previamente informado. Por exemplo, se o paciente manifestou o desejo de ser acessado apenas por e-mail, ele não pode receber ligações ou mensagens de texto da instituição.

3 - **Necessidade** – Os dados devem ter o uso limitado ao necessário para o alcance de objetivos pré-estabelecidos. Ou seja, as empresas devem coletar apenas aquelas informações estritamente necessárias para prestação dos seus serviços. Por exemplo, caso o objetivo seja disparar e-mails, é desnecessário solicitar o número do telefone ou endereço do paciente.

4 - **Livre acesso** – Os titulares dos dados devem sempre ter acesso fácil e gratuito às suas informações, além de serem informados sobre como essas informações serão utilizadas e qual será a duração desse processo. Por exemplo, um paciente cadastrado em uma base de dados há seis meses, pode decidir revisar as informações ou excluir dados que não queira mais compartilhar com a organização.

5 - **Qualidade dos dados** – Princípio que garante aos titulares que seus dados serão exatos, terão informações claras, relevantes e atualizadas para tratamento. Por exemplo, se o paciente, cadastrado em uma base de dados há algum tempo, notou que as informações estão desatualizadas, poderá solicitar alteração a qualquer momento.

6 - **Transparência** – Garante aos usuários informações claras e de fácil acesso sobre o tratamento de seus dados e quem são os responsáveis por tratá-los. Por exemplo, ao receber um SMS de um hospital falando sobre uma nova unidade de atendimento na região onde mora, o paciente pode questionar o motivo para que tenha recebido essa mensagem e qual critério utilizaram para selecioná-lo.

7 - **Segurança** – As empresas que tratam de dados devem adotar medidas para proteger as informações de acessos não autorizados, eventos acidentais, alteração, perda, comunicação ou compartilhamento irregular. Por exemplo, o paciente informou o número do seu CPF ou Seguro de Saúde para realizar um procedimento. É responsabilidade da empresa proteger esses dados para que esse usuário não seja prejudicado por fraudes.

8 - Prevenção – É importante adotar medidas para prevenir a ocorrência de danos no tratamento das informações. Em caso de invasão ao sistema em que os dados estão armazenados, por exemplo, a empresa detentora de dados de cidadãos brasileiros será responsabilizada por qualquer uso indevido das informações que estavam em seu poder.

9 - **Não discriminação** – Os dados não podem ser utilizados para a promoção de ações ilícitas,

discriminatórias ou abusivas. Por exemplo, o tabelamento do mesmo serviço por preços diferentes, considerando a região de residência do cliente, que foi identificada no banco de dados, é uma prática considerada inadequada.

10 - **Responsabilização e prestação de contas** – As organizações são responsáveis pelos dados que detém e, por essa razão, têm o dever de informar quando terceiriza o tratamento das informações, bem como identificar o encarregado pela tarefa. Dessa forma, a empresa deve a possuir documentação que comprove a regularidade do processo, em concordância com a lei.

Não tenha dúvida sobre a importância da LGPD

Quando uma empresa estabelece contato com diferentes stakeholders, essas pessoas fornecem seus dados pessoais. Então, preserve essa relação de confiança. O vazamento dos dados ou uso inadequados deles podem, em alguns casos, gerar danos irreparáveis aos envolvidos. Somente isso já é um forte argumento para se tornar um adepto da LGPD.

A nova lei dará segurança jurídica às pessoas, enquanto gradativamente irá extinguir as práticas ilegais com relação ao uso de dados dos cidadãos, como o cookie pool e a venda de lista de dados. A ideia é que, com o tempo, o Brasil possa ser visto como referência na segurança de dados e, assim, atrair parcerias internacionais de países que também prezam pelas boas práticas relacionadas aos dados dos cidadãos.

Não adquira qualquer dado sem consentimento

A LGPD exige que o consentimento para o uso de dados pessoais ou recebimento de conteúdos, promoções e informações seja fornecido por meio de formulário físico ou eletrônico, que pode ser um canal de opt-in, check-box ou outro da preferência da companhia. Mas, é fundamental poder comprovar esse “ok” em caso de fiscalização. Vale ressaltar, que é considerada falta grave ações que induzam a pessoa ao consentimento ou que sejam caracterizadas como coação. Deve-se prezar pelo livre direito de escolha do cidadão.

As organizações devem ficar atentas, também para não cometer outras três falhas:

● Formulário de consentimento com frases genéricas – Não será aceita pela LGPD frases que digam algo, como “autorizo o livre uso de meus dados de saúde para fins de pesquisa”. É preciso informar qual será a pesquisa, a que se destina, a quem beneficiará, quais pessoas terão acesso aos dados, quando e como será divulgada, entre outros detalhes.

● Impedir que o cliente peça a exclusão de seus dados da lista – Opte por criar um mecanismo que facilite o descadastramento do cliente da base de dados, em uma ação simples, sem burocracias e com a garantia de atendimento imediato à solicitação.

● Ocultar do cliente informações sobre mudanças nos processos – É direito do cliente ser informado sobre qualquer mudança nos processos de coleta, tratamento ou armazenamento dos dados. Inclusive, neste caso, é importante reforçar a ele a possibilidade de solicitar o descadastro da base de dados, caso não concorde com algo da nova política. Dessa forma, dedique atenção para estruturar as práticas de adequação à LGPD e, para evitar ferir as normas da lei, só faça alterações nos processos caso elas sejam fundamentais para o negócio.

Atenção especial aos dados de jovens

No contato com jovens com idade inferior a 12 anos, a LGPD exige um cuidado extra com relação à manipulação dos dados. As informações de membros desse público só podem ser coletadas mediante a autorização dos respectivos responsáveis legais. É importante lembrar, também, que a forma de comunicação com o cliente deve considerar o perfil do público. Isso quer dizer que, ao falar com uma criança ou jovem, não é permitido usar termos jurídicos ou qualquer outra linguagem de difícil interpretação e compreensão.

Setor de saúde, um dos mais sensíveis

Em geral, a área mais sensível da vida das pessoas é a saúde. Isso faz com que, nas instalações de clínicas, hospitais e laboratórios, qualquer exposição de informações sobre os pacientes sejam cuidadosamente planejadas. Esse cuidado deve ser redobrado com a chegada da LGPD. A orientação diz respeito, por exemplo, a placas de identificação na porta do quarto ou na cabeceira e pés do leito. Há também a necessidade de maior fiscalização quanto a dados do prontuário físicos ou virtuais para que não haja ações que caracterizem vazamento de dados. Algumas medidas preventivas são importantes:

● Só exponha ou utilize informações do paciente nas instalações da organização caso tenha autorização formal dele;

● Treine a equipe com relação à deveres, direitos e punições relacionadas à LGPD;

● Mapeie, categorize e monitore as informações de pessoas que circulam na instituição;

● Invista em soluções de segurança dos dados coletados; e

● Mantenha o constante monitoramento das ações e revisão dos processos.

As empresas que não respeitarem as diretrizes da LGPD estarão sujeitas a multas simples ou diárias de até 2% do faturamento da empresa, limitado a R$ 50 milhões por infração. Além disso, também poderão ter os dados irregulares bloqueados para o uso ou a infração amplamente divulgada.

Em tempos de desejo de retomada da economia, não é inteligente perder dinheiro, clientes ou a credibilidade. Sairão na frente as organizações que aproveitarem os próximos meses para se adequarem, seja buscando o apoio de especialistas ou aderindo a ferramentas que facilitem o processo.

(*) **Guilherme Ferri** e **Ricardo Medina**, Managing Partner da MF Marketing and Business Advisors.

Fonte: Saúde Business, em 29.05.2019.