Perguntas e respostas sobre a LGPD na área da saúde

Maria Celeste Osório Wender[1], Lia Cruz Vaz da Costa Damásio[2]

1. Diretora de Defesa e Valorização Profissional da Febrasgo.
2. Membro da Comissão Nacional de Defesa e Valorização Profissional; médica e advogada.

O QUE É A LGPD?

LGPD é a sigla para Lei Geral de Proteção de Dados, a Lei nº 13.709/2018, que regulamenta a maneira pela qual os dados pessoais são utilizados por pessoas ou empresas, criando exigências para o seu tratamento, que inclui sua coleta, utilização, armazenamento e eliminação no meio físico e digital.[1,2]

QUAL A FINALIDADE DA LGPD?

A LGPD tem por finalidade regulamentar o uso, a proteção e a transferência de dados pessoais no território brasileiro.[2] No nosso dia a dia, preenchemos fichas cadastrais e, como médicos ou empresa, solicitamos vários dados e fornecemos e acessamos esses dados pessoais em diversas situações, tais como inscrição em cursos, realização de compras pela internet, participação em pesquisas nas redes sociais, atendimentos médicos, realização de exames, entre outras. E o que é feito com nossas informações? De que forma são utilizadas? São repassadas para terceiros? Nesse cenário, em que há grande troca de informações, sobretudo no ambiente digital, entra em vigor a LGPD – Lei nº 13.709/2018 –, que surge com a finalidade de criar regras para proteger os direitos fundamentais de liberdade e de privacidade e a livre formação da personalidade de cada indivíduo.[2,3]

A informação se tornou um dos bens mais preciosos e valorizados para a humanidade.[4] A exemplo do que está sendo realizado em diversos países, a LGPD foi inspirada no Regulamento Geral sobre a Proteção de Dados da União Europeia e publicada com a finalidade de criar um ambiente de segurança jurídica por meio da padronização de normas e práticas para a proteção, de forma igualitária, de dados pessoais no Brasil.[3]

O QUE SÃO OS DADOS PESSOAIS CITADOS NA LGPD?

Para efeitos da lei, se uma informação permite identificar, direta ou indiretamente, um indivíduo que esteja

vivo, então ela é considerada um dado pessoal: nome, RG, CPF, gênero, data e local de nascimento, telefone, endereço residencial, localização via GPS, retrato em fotografia, prontuário de saúde, cartão bancário, renda, histórico de pagamentos, hábitos de consumo, preferências de lazer, endereço de IP (protocolo da internet) e *cookies*, entre outros.[3]

QUAIS SÃO OS DADOS CLASSIFICADOS COMO SENSÍVEIS?

Um dado pessoal é classificado como sensível pela LGPD quando se trata de 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.[2] Há maiores restrições no uso e coleta de dados sensíveis.[2]

QUANDO OS DADOS SENSÍVEIS PODEM SER UTILIZADOS?

Os dados sensíveis também podem ser tratados se tiverem o consentimento explícito da pessoa e uma finalidade definida; e, sem o consentimento do titular, quando forem indispensáveis em situações ligadas a: uma obrigação legal; políticas públicas; estudos via órgão de pesquisa; um direito, em contrato ou processo; preservação da vida e da integridade física de uma pessoa; tutela de procedimentos feitos por profissionais das áreas da saúde ou sanitária; prevenção de fraudes contra o titular.[3]

O QUE SERIAM OS DADOS ANONIMIZADOS E PSEUDONIMIZADOS E QUAL SUA SUJEIÇÃO À LGPD?

A anonimização é a utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo.[2] Os dados anonimizados são aqueles que, originariamente, eram relativos a uma pessoa, mas que passaram por etapas que garantiram a desvinculação deles dessa pessoa.[3] Se um dado for anonimizado, então a LGPD não se aplicará a ele.[5] Vale frisar que um dado só é considerado efetivamente anonimizado se não permitir que, via meios técnicos e outros, se reconstrua o caminho para "descobrir" quem era a pessoa titular do dado – se de alguma forma a identificação ocorrer, então ele não é, de fato, um dado anonimizado, e sim apenas um dado pseudonimizado e estará, então, sujeito à LGPD (Fonte: https://www.serpro.gov.br/lgpd/menu/protecao-de-dados). Dados pseudonimizados são aqueles dados que também passaram por etapas de tratamento, em que se permitiu trocar o conjunto de dados originais (por exemplo, o *e-mail* do titular dos dados ou o próprio nome) por um pseudônimo. Ou seja, neste caso é possível identificar quem era a pessoa titular do dado, sujeitando-se à LGPD.

O QUE É O TRATAMENTO DE DADOS PESSOAIS?

É toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.[2] Considera-se, assim, tratamento de dado toda e qualquer atividade que utilize dados pessoais na execução da sua operação. A lei menciona 20 ações relacionadas ao tratamento de dados:[3]

- **Acesso:** ato de ingressar, transitar, conhecer ou consultar a informação, bem como possibilidade de usar os ativos de informação de um órgão ou entidade, observada eventual restrição que se aplique;
- **Armazenamento:** ação ou resultado de manter ou conservar em repositório um dado;
- **Arquivamento:** ato ou efeito de manter registrado um dado, embora já tenha perdido a validade ou esgotado a sua vigência;
- **Avaliação:** análise do dado com o objetivo de produzir informação;
- **Classificação:** maneira de ordenar os dados conforme algum critério estabelecido;
- **Coleta:** recolhimento de dados com finalidade específica;
- **Comunicação:** transmissão de informações pertinentes a políticas de ação sobre os dados;
- **Controle:** ação ou poder de regular, determinar ou monitorar as ações sobre os dados;
- **Difusão:** ato ou efeito de excluir, propagação, multiplicação dos dados;
- **Distribuição:** ato ou efeito de dispor de dados de acordo com algum critério estabelecido;
- **Eliminação:** ato ou efeito de excluir ou destruir dados do repositório;
- **Extração:** ato de copiar ou retirar dados do repositório em que se encontrava;
- **Modificação:** ato ou efeito de alterar o dado;
- **Processamento:** ato ou efeito de processar dados visando organizá-los para obtenção de um resultado determinado;
- **Produção:** criação de bens e de serviços a partir do tratamento de dados;
- **Recepção:** ato de receber os dados ao final da transmissão;
- **Reprodução:** cópia de dado preexistente obtido por meio de qualquer processo;
- **Transferência:** mudança de dados de uma área de armazenamento para outra, ou para terceiro;

- **Transmissão:** movimentação de dados entre dois pontos por meio de dispositivos elétricos, eletrônicos, telegráficos, telefônicos, radioelétricos, pneumáticos etc.; e
- **Utilização:** ato ou efeito do aproveitamento dos dados.

NA PRÁTICA MÉDICA, PODEMOS REALIZAR O TRATAMENTO DE DADOS PESSOAIS REFERIDO NA LGPD?

A LGPD possibilita a hospitais, médicos, laboratórios, centros de diagnóstico, planos e seguros de saúde e demais empresas e profissionais da área da saúde o tratamento de dados pessoais, desde que referidas empresas e/ou pessoas consigam enquadrar o processo de tratamento em uma das bases legais do artigo 7º da referida lei.[2]

São 10 as bases legais que permitem o tratamento de dados pessoais:[2,6]

1. Consentimento informado do paciente, que é o titular dos dados pessoais;
2. Cumprimento de obrigação legal ou regulatória pelo profissional ou serviço de saúde;
3. Execução de políticas públicas;
4. Realização de estudos por órgãos de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
5. Execução de contrato;
6. Exercício de direito em processo judicial, administrativo ou arbitral;
7. Proteção da vida;
8. Tutela da saúde;
9. No legítimo interesse do controlador; e
10. Para proteção do crédito.

A regra, portanto, é a seguinte: somente será permitido o tratamento de dados pessoais se esse se encaixar em pelo menos uma das 10 bases legais acima e se essa base legal encontrada atender aos seguintes requisitos, sem exceção de nenhum deles:

I – **Finalidade:** realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

II – **Adequação:** compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

III – **Necessidade:** limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

IV – **Livre acesso:** garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

V – **Qualidade dos dados:** garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

VI – **Transparência:** garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

VII – **Segurança:** utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

VIII – **Prevenção:** adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

IX – **Não discriminação:** impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

X – **Responsabilização e prestação de contas:** demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

Com isso, temos que o estabelecimento de saúde, além de encontrar a base legal que autoriza o tratamento do dado pessoal em questão, deverá demonstrar que o tratamento atende a todos os 10 requisitos acima.[2,4]

Vale ressaltar, ainda, que os dados relativos à saúde são dados sensíveis que exigem um tratamento mais cauteloso, devendo o consentimento obtido do titular dos dados, além de conter toda a informação possível, ser específico sobre a finalidade do tratamento. Aqui o foco da lei é evitar que o titular dos dados seja vítima de algum tipo de discriminação em decorrência de uma doença grave ou transmissível, por exemplo.[4]

De qualquer modo, mesmo se o estabelecimento de saúde não tiver o consentimento informado e específico do titular sobre quais dados coletará e como e por que procederá ao tratamento desses dados, esse ainda assim poderá ocorrer em algumas hipóteses, desde que se adeque a uma das outras nove bases legais, como, por exemplo, num caso de emergência em que o próprio paciente (titular dos dados pessoais) não possa fornecer o consentimento, mas existe a base legal de proteção da vida.[4]

COMO DEVE SER DADO O CONSENTIMENTO PARA O TRATAMENTO DOS DADOS PESSOAIS?

O consentimento previsto no inciso I do art. 7º da LGPD deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular e deve ser dada especial atenção aos parágrafos do artigo sobre o consentimento:

§ 1º Caso o consentimento seja fornecido por escrito, esse deverá constar de cláusula destacada das demais cláusulas contratuais.

§ 2º Cabe ao controlador o ônus da prova de que o consentimento foi obtido em conformidade com a Lei.

§ 3º É vedado o tratamento de dados pessoais mediante vício de consentimento.

§ 4º O consentimento deverá referir-se a finalidades determinadas, e as autorizações genéricas para o tratamento de dados pessoais serão nulas, ou seja, não valem as expressões "para todos os fins, para os devidos fins etc.".

§ 5º O consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação, nos termos do inciso VI do *caput* do art. 18 desta Lei.

§ 6º Em caso de alteração de informação ou uso da informação, o paciente titular dos dados deverá ser informado, podendo, nos casos em que o seu consentimento é exigido, revogá-lo caso discorde da alteração.

Dono do dado pessoal, o titular tem a prerrogativa de autorizar, negar ou reconsiderar o uso de suas informações. O consentimento pode ser manifestado por escrito ou por qualquer outro meio que demonstre, de forma clara e inequívoca, que suas informações podem ser usadas por empresas e órgãos públicos. O consentimento pode ser tácito quando o titular o torna manifestamente público previamente. Não há exigência de consentimento nos casos em que o dado for indispensável para: o cumprimento de uma obrigação legal; a execução de política pública prevista em lei; a realização de estudos por órgãos de pesquisa; a execução de contratos; a defesa de direitos em processo; a preservação da vida e da integridade física de uma pessoa; a tutela de ações feitas por profissionais das áreas da saúde ou sanitária; a prevenção de fraudes contra o titular; a proteção do crédito; ou o atendimento a um interesse legítimo, que não fira direitos fundamentais do cidadão.[3]

QUAIS AS POSSÍVEIS SANÇÕES NO CASO DE INFRAÇÃO ÀS REGRAS DA LGPD?

Falhas de segurança podem ocasionar multas de até 2% do faturamento anual da organização, no limite de R$ 50 milhões de reais por infração. Caberá à Autoridade Nacional de Proteção de Dados (ANPD) fixar níveis de penalidade segundo a gravidade da falha e enviar alertas e orientações antes de aplicar as sanções.[3]

As sanções previstas em caso de infrações às regras da LGPD são:[2]

- Advertência com indicação de prazo para adoção de medidas corretivas;
- Multa simples, de até 2% do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50 milhões de reais por infração;
- Multa diária, observado o limite total de R$ 50 milhões de reais por infração;
- Publicização da infração após devidamente apurada e confirmada a sua ocorrência;
- Bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
- Eliminação dos dados pessoais a que se refere a infração;
- Suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de seis meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador;
- Suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de seis meses, prorrogável por igual período; e
- Proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

A lei é extremamente severa com o uso indevido de dados e, no ambiente da saúde, regulou situações até então corriqueiras, proibindo-as daqui por diante, como a tratada no art. 11, § 5º, em que as operadoras de planos privados de assistência à saúde realizem o tratamento de dados de saúde para a prática de seleção de riscos na contratação de qualquer modalidade, assim como na contratação e exclusão de beneficiários.

QUANDO ENTRA EM VIGOR A LGPD?

A data da publicação da LGPD é 14 de agosto de 2018. De acordo com o Diário Oficial, a vigência da lei, em relação à criação – pela Lei nº 13.853, de 8 de julho de 2019 – da ANPD e do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (CNPD), é a partir de 28/12/2018;[7] em relação aos princípios, fundamentos e requisitos so-

bre os dados e tratamento dos dados, já estão em vigor desde 14 de agosto de 2020, e em relação aos artigos 52, 53 e 54 (efetivação da aplicação das sanções pela ANPD), a data prevista para o início da vigência é 1º/8/2021.

QUAIS IMPLICAÇÕES PRÁTICAS DA LGPD NA ÁREA DA SAÚDE?

É relevante que toda empresa e profissional que atue no setor de atendimento à saúde observe, quando da implementação dos programas de conformidade, as normas aplicáveis ao seu ramo de atuação e de que forma elas se comunicam com as exigências da LGPD.[1]

Citam-se alguns exemplos do impacto da LGPD na área da saúde:[8]

- Os dados pessoais de um paciente somente poderão ser coletados, armazenados e processados em sistemas de informação em saúde com seu expresso consentimento livre e esclarecido (inclusive dados retroativos, ou seja, todos os pacientes já armazenados nos sistemas, ou seus responsáveis, terão que ser solicitados novamente);
- Os pacientes terão o direito de saber para que, quando e por quem os seus dados foram utilizados e poderão restringir o direito de acesso a quem desejarem (inclusive grupos de usuários dos sistemas). Ou seja, terão acesso às trilhas de auditoria (*logs*) e a todos os dados armazenados, podendo, a qualquer momento, suspender seu consentimento ou pedir o apagamento completo ou parcial dos dados pessoais (inclusive demográficos);
- Os dados pessoais terão que ser anonimizados e deverão ser criptografados;
- Todas as transmissões entre sistemas terão que ser criptografadas;
- Todas as empresas e instituições que armazenam dados identificados de pessoas terão que ter políticas registradas, um sistema de gestão de segurança de informação e pelo menos um gestor responsável;
- Os *softwares* terão que implementar massivas e complexas formas de proteção de dados contra vários tipos de roubo de identidade, de bancos de dados, de transações etc., inclusive para sistemas baseados em nuvens;
- Deve-se ter cautela com a adequação e o "excesso de segurança", que poderia prejudicar uma tendência fundamental para os prontuários eletrônicos, que é a interoperabilidade (troca de informações) entre sistemas heterogêneos e também a elaboração de dados agregados, como no Datasus, ou levar a situações esdrúxulas, como um paciente necessitando de cuidados emergenciais não poder ser atendido em virtude dos seus dados estarem com acesso vetado, o que reforça a necessidade de atenção e individualização na adequação de cada serviço às regras da LGPD.

São profundas e numerosas as mudanças trazidas pela LGPD, exigindo uma mudança de postura de todos nós, que estamos habituados a tratar dados pessoais e, no caso da medicina, muitos dados sensíveis, sem muitas exigências. Contudo, embora desafiador, o resultado da LGPD, bem estabelecido na sociedade, é, acima de tudo, uma mudança cultural importante e necessária em relação ao cuidado com os dados pessoais nas atividades cotidianas. Ainda há muitas indefinições quanto às ações da ANPD e do CNPD, bem como dos efetivos mecanismos que serão utilizados para a fiscalização e cobranças das ações e possíveis sanções.

A Febrasgo permanecerá atenta às novidades e atualizações sobre a efetivação e fiscalização da LGPD e seus impactos na prática médica e, desde já, recomenda fortemente a leitura atenta da lei e a observância do fluxo dos dados pessoais em sua prática diária para se adequar às exigências da LGPD.

REFERÊNCIAS

1. Sarnick SR. Os desafios da implementação da LGPD na área da Saúde [Internet]. 2021 [cited 2021 Feb 17]. Available from: https://www.saudebusiness.com/legislao-e-regulamentao/os-desafios-da-implementao-da-lgpd-na-rea-da-sade
2. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet) [Internet]. 2018 [cited 2021 Mar 1]. Available from: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm
3. Agência Nacional de Saúde Suplementar (ANS). LGPD: informações básicas para entender a Lei Geral de Proteção de Dados Pessoais. Rio de Janeiro: ANS; 2020 [cited 2021 Feb 21]. Available from: http://www.ans.gov.br/images/stories/acessoainformacao/Cartilha_LGPD_r2.pdf
4. Fattori M. #LGPD na saúde: o tratamento de dados pessoais no pronto socorro. Como médicos, clínicas, laboratórios, hospitais, planos e seguros de saúde devem agir? [Internet]. 2021 [cited 2021 Feb 21]. Available from: https://www.seusdados.com/lgpd-na-saude-o-tratamento-de-dados-pessoais-no-pronto-socorro-como-medicos-clinicas-laboratorios-hospitais-planos-e-seguros-de-saude-devem-a/
5. Agência Nacional de Saúde Suplementar (ANS). Conheças as ações da ANS para a implementação da LGPD [Internet]. 2021 [cited 2021 Feb 21]. Available from: http://www.ans.gov.br/aans/noticias-ans/sobre-a-ans/6195-conheca-as-acoes-da-ans-para-a-implementacao-da-lgpd
6. Guia de Boas Práticas – Lei Geral de Proteção de Dados (LGPD) [Internet]. 2020 [cited 2021 Feb 21]. Available from: https://www.gov.br/governodigital/pt-br/governanca-de-dados/guia-de-boas-praticas-lei-geral-de-protecao-de-dados-lgpd
7. Lei nº 13.853, de 8 de julho de 2019. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências [Internet]. 2019 [cited 2021 Feb 21]. Available from: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13853.htm
8. Como a LGPD irá afetar as informações de saúde? [Internet]. 2018 [cited 2021 Feb 21]. Available from: https://www.delphos.com.br/como-a-lgpd-ira-afetar-as-informacoes-de-saude/