DOI: https://doi.org/10.11606/issn.2316-9044.rdisan.2021.168023 Artigo Original

Marcos César Botelho[1]
Elimei Paleari do Amaral Camargo[2]

A APLICAÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS NA SAÚDE

The application of the General Data Protection Law in health

[1]Universidade Estadual do Norte do Paraná. Jacarezinho/PR, Brasil.
[2]Universidade Federal de Rondônia. Cacoal/RO, Brasil.

Correspondência: Marcos César Botelho. *E-mail*: marcos.botelho@uenp.edu.br

Recebido: 23/03/2020. Aprovado: 13/10/2020.

RESUMO

Motivado pela adoção do Regulamento Geral sobre a Proteção de Dados pela União Europeia, o legislador brasileiro aprovou a Lei Geral de Proteção de Dados, expressamente tornando a proteção de dados pessoais um direito fundamental e reconhecendo a existência de uma categoria de dados específica, denominada de dados pessoais sensíveis, cujo conceito abarca os dados relativos à saúde e que recebem tratamento específico desse diploma legal. O objetivo do presente estudo foi analisar como a Lei Geral de Proteção de Dados trata a proteção de dados relativos à saúde. Para tanto, utilizando método dedutivo e análise bibliográfica, o estudo foi dividido em duas partes. Na primeira foi exposto o conceito jurídico de dados trazido pela Lei Geral de Proteção de Dados, bem como a definição legal de dados sensíveis. Na segunda parte discutiu-se como essa lei trata os dados relativos à saúde. De modo geral, conclui-se que, com a entrada em vigor da Lei Geral de Proteção de Dados, profissionais da saúde, clínicas médicas, hospitais e centros de saúde, entre outros, que realizarem tratamento de dados pessoais sensíveis relacionados à saúde deverão adotar medidas para adaptar tais atividades à legislação o mais brevemente possível, a fim de evitar sanções que podem ir desde a aplicação de multas pecuniárias até a proibição do uso de dados pessoais sensíveis.

Palavras-Chave

Dados Pessoais Sensíveis; Lei Geral de Proteção de Dados; Saúde; Segurança da Informação.

ABSTRACT

Motivated by the adoption of the General Data Protection Regulation by the European Union, the Brazilian legislator approved the General Data Protection Law, expressly making the protection of personal data a fundamental right and recognizing the existence of a specific category of data, known as sensitive personal data, the concept of which encompasses data relating to health and which receive specific treatment in this legal document. The objective of the present study was to analyze how the General Data Protection Law deals with the protection of health-related data. To this end, using a deductive method and bibliographic analysis, the study was divided into two parts. In the first part, the legal concept of data brought by the General Data Protection Law was exposed, as well as the legal definition of sensitive data. The second part discussed how this law deals with health data. In general, it is concluded that, with the entry into force of the General Data Protection Law, health professionals, medical clinics, hospitals and health centers, among others, who process sensitive personal data related to health should adopt measures to adapt their activities to the legislation as soon as possible, in order to avoid sanctions that can range from the imposition of financial fines to the prohibition of the use of sensitive personal data.

Keywords

Sensitive Personal Data; General Data Protection Law; Health; Information Security.

Introdução

A sociedade digital gerou oportunidades para diversas áreas de negócio a partir da valorização de um ativo imprescindível para o êxito das organizações contemporâneas: o dado. Fenômenos como o *big data* e a datificação ressaltam a importância que os dados e as informações assumiram nos negócios modernos, ao mesmo tempo em que revelam os perigos à intimidade, à privacidade e à própria dignidade humana com a exposição e o uso de dados pessoais sem qualquer controle de seu titular.

Nesse contexto, surgiram regulamentos visando a disciplinar o tratamento de dados pessoais, primeiramente na Europa, com o Regulamento Geral sobre a Proteção de Dados, aprovado em 2016 e em vigor desde maio de 2018. No Brasil, a Lei n. 13.709[1], de 14 de agosto de 2018, a chamada Lei Geral de Proteção de Dados (LGPD), entrou em vigor em agosto de 2020, alterada em parte pela Lei n. 13.853/2019[2].

Dessa forma, o Brasil entrou para o grupo de países que contam com normas protetivas no que se refere à coleta e manipulação de dados pessoais, reconhecendo a natureza fundamental do direito a essa proteção.

A LGPD assume que há uma categoria própria de dados pessoais, denominada dados sensíveis e que demanda uma proteção mais específica e rigorosa. A lei enquadra os dados relativos à saúde nessa categoria.

O objetivo do presente estudo foi analisar o tratamento conferido pela LGPD à proteção de dados relativos à saúde. Para tanto, o estudo foi dividido em duas partes. Na primeira, apresenta-se o conceito jurídico de dados trazido pela LGPD, bem como a definição legal de dados sensíveis. Na segunda parte, discute-se o tratamento que a LGPD dá aos dados relativos à saúde, em dois tópicos: o tratamento dos dados referentes à saúde previsto no artigo 11, inciso II, alínea *f*; e o tratamento de dados pessoais para fins de estudos em saúde pública, previsto no artigo 13.

I. Dados pessoais e dados sensíveis na LGPD

Não existem dúvidas de que os dados e as informações estão em um patamar de fundamental importância para as organizações contemporâneas. Considerados o "novo petróleo", os dados são um ativo relevante para as atividades econômicas, e sua manipulação e sua utilização são fatores determinantes para o êxito da atividade econômica. Ou seja, "[...] os dados se tornaram matéria-prima dos negócios, um recurso econômico vital, usado para criar uma nova forma de valor econômico"[3].

---

[1]BRASIL. *Lei n. 13.709, de 14 de agosto de 2018*. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 16 nov. 2021.
[2]BRASIL. *Lei n. 13.853, de 8 de julho de 2019*. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13853.htm#art1. Acesso em: 16 nov. 2021.
[3]MAYER-SCHÖNBERGER, Viktor; CUKIER, Kenneth. *Big data:* como extrair volume, variedade, velocidade e valor da avalanche de informação cotidiana. Rio de Janeiro: Elsevier, 2013. p. 4.

A produção de dados tem alcançado números expressivos. Basta dizer que, no ano de 1986, cerca de 40% de toda a capacidade computacional do mundo existia na forma de calculadoras de bolso, com um poder de processamento muito superior à de todos os computadores da época, produzindo-se, assim, pouca informação digital; já em 2020, foi alcançada a impressionante marca de 44 zettabytes de informações digitais produzidas. Mayer-Schönberger e Cukier lembram que a quantidade de informação armazenada cresce quatro vezes mais rápido do que a economia mundial, e a capacidade de processamento dos computadores cresce nove vezes mais rápido[4].

Para compreender esse contexto, faz-se necessário entender os conceitos de dado, informação e conhecimento. Embora sejam expressões muitas vezes utilizadas como sinônimas, no âmbito da tecnologia da informação expressam realidades distintas, embora conectadas.

Os dados representam o fato bruto, o elemento básico; trata-se dos fatos que são coletados e armazenados, podendo se apresentar em formato eletrônico analógico ou digital[5]. Desta forma, o dado em si possui pouco valor agregado e depende de um processo de tratamento para a extração de algum significado a fim de ser útil em determinado contexto.

Segundo Goldschmidt, Passos e Bezerra:

> Os dados [...] podem ser interpretados como itens elementares, captados e armazenados por recursos da Tecnologia da Informação. São cadeias de símbolos e não possuem semântica (*i.e.*, significado). Seu propósito é expressar fatos do mundo real de forma a serem tratados no contexto computacional[6].

A informação, por seu turno, expressa dados que foram devidamente processados e analisados e que possuam um significado em determinado contexto[7]. Portanto, o tratamento dos dados gera utilidade, além de agregar valor, auxiliando a tomada de decisões.

Segundo Stair e Reynolds:

> O tipo de informação criada depende das relações definidas entre os dados existentes [...]. O acréscimo de dados novos ou diferentes indica que relações podem ser redefinidas e novas informações podem ser criadas[8].

---

[4]MAYER-SCHÖNBERGER, Viktor; CUKIER, Kenneth. *op. cit.*, p. 6.
[5]AMARAL, Fernando. *Introdução à ciência de dados*. Rio de Janeiro: Alta Books, 2016. p. 3.
[6]GOLDSCHMIDT, Ronaldo; PASSOS, Emmanuel; BEZERRA, Eduardo. *Data mining:* conceitos, técnicas, algoritmos, orientações e aplicações. 2. ed. Rio de Janeiro: Elsevier, 2015. p. 3.
[7]HINTZBERGEN, Jule *et al*. *Fundamentos de segurança da informação*: com base na ISSO 27001 e na ISSO 27002. Rio de Janeiro: Brasport, 2018. p. 53.
[8]STAIR, Ralph M.; REYNOLDS, George W. *Princípios de sistemas de informação*. Tradução da 6. ed. americana. São Paulo: Pioneira Thomson Learning, 2006. p. 5.

Por fim, o tratamento de dados que resulta na informação permite a obtenção de conhecimento, "[...] que corresponde a um padrão ou conjunto de padrões cuja formulação pode envolver e relacionar dados e informações"[9]. Para Stair e Reynolds, "conhecimento é a consciência e o entendimento de um conjunto de informações e formas de torná-las úteis para apoiar uma tarefa específica ou tomar uma decisão"[10].

É nesse contexto que fenômenos como a dataficação e o *big data* estão inseridos. Aliada a outro fenômeno, o da Internet das Coisas (IoT, na sigla em inglês), a produção massiva de dados é uma realidade incontestável, com consequências tanto positivas quanto negativas.

A dataficação, enquanto um processo que transforma todos os aspectos da vida em dados[11], demonstra que, na sociedade da informação, nosso comportamento no ambiente virtual sempre irá produzir dados e gerar trilhas digitais sobre as quais muitas vezes não temos conhecimento, tampouco controle.

Segundo Amaral:

> Do ponto de vista tecnológico, o elemento principal associado ao *Big Data* é o registro de qualquer fenômeno, natural ou não, em dados. Esses dados são persistidos, armazenados para reprodução ou análise, sendo imediata ou futura. Tal fenômeno é conhecido como *datafication*. Em outras palavras, *datafication* é o registro eletrônico de um fenômeno qualquer[12].

Essa produção massiva de dados tem grande potencial lesivo quando se fala em dados pessoais. O advento da IoT, com a conexão de bilhões de dispositivos à internet, faz com que a produção de dados pessoais adquira grande importância nos cenários jurídico, econômico e social.

Eventos recentes de vazamento de dados pessoais de inúmeras pessoas no mundo – como o caso envolvendo a empresa Cambridge Analytica, em que o vazamento de dados pessoais de 75 milhões de usuários do *Facebook* serviu de sinal de alerta às autoridades – culminaram na aprovação, em 2016 pela União Europeia, do Regulamento Geral sobre a Proteção de Dados Pessoais, cujo:

> [...] foco é a proteção de direitos e garantias fundamentais dos cidadãos, com o objetivo de mitigar os riscos, em relação ao que pode ser levado a efeito, a partir da coleta e do futuro uso, compartilhamento, armazenamento, entre outros desse dados[13].

---

[9] GOLDSCHMIDT, Ronaldo; PASSOS, Emmanuel; BEZERRA, Eduardo. *op. cit.*, p. 3.
[10] STAIR, Ralph M.; REYNOLDS, George W. *op. cit.*, p. 5.
[11] SCHUTT, Rachel; O'NEIL, Cathy. *Doing data science*. Sebastopol: O'Reilly Media, 2014. p. 5.
[12] AMARAL, Fernando. *op. cit.*, p. 9.
[13] MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (Coords). *Comentários ao GDPR:* Regulamento Geral de Proteção de Dados da União Europeia. São Paulo: Editora Revista dos Tribunais, 2018. p. 24.

O Brasil, seguindo a tendência estabelecida pela União Europeia, aprovou a Lei n. 13.709/2018 (Lei Geral de Proteção de Dados, LGPD), que dispõe sobre o tratamento de dados pessoais nos meios físico ou digital por pessoa natural ou pessoa jurídica de direito público ou privado.

Segundo o artigo 1º da LGPD,seu desiderato é a proteção dos direitos fundamentais à liberdade e à privacidade, além do livre desenvolvimento da personalidade da pessoa natural. Objetiva-se, portanto, a proteção daqueles dados e informações que permitam a identificação da pessoa natural. Vale destacar o que prescreve o artigo 5º desse diploma legal: "Para fins desta Lei, considera-se: I – dado pessoal: informação relacionada a pessoa natural identificada ou identificável".

A partir do conceito jurídico de dado pessoal, é fácil constatar que ele abrange tanto o dado em sentido estrito quanto a informação. Enquanto aquele é o fato bruto, com pouco valor agregado, a informação consiste no resultado do tratamento de dados. Logo, para os fins perseguidos pela LGPD, a proteção recai tanto sobre os dados como sobre as informações que estejam relacionadas à pessoa natural que seja identificada ou identificável.

A ideia de adotar um conceito que abarque tanto o dado em sentido estrito quanto a informação não é nova no ordenamento jurídico brasileiro. Por exemplo, a Lei n. 12.527/2011[14], que disciplina o acesso à informação, define informação como "dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato" (art. 4º, I) e informação pessoal como "aquela relacionada à pessoa natural identificada ou identificável" (art. 4º, IV).

Da definição apresentada no artigo 5º, inciso I da LGPD, é possível constatar que o diploma normativo adotou o critério expansionista, na medida em que os dados pessoais são aqueles que permitem identificar imediata ou mediatamente a pessoa natural. Ou seja, a legislação "[...] abarcou também os dados que tornam a pessoa identificável de forma não imediata ou direta"[15].

A LGPD, contudo, alude a uma categoria específica de dados, os chamados **dados sensíveis**. Sua definição vem estampada no inciso II do artigo 5º:

---

[14] BRASIL. *Lei n. 12.527, de 18 de novembro de 2011*. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 16 nov. 2021.

[15] COTS, Márcio; OLIVEIRA, Ricardo. *Lei Geral de Proteção de Dados Pessoais comentada*. 2. ed. São Paulo: Editora Revista dos Tribunais, 2019. p. 71. Oposto ao critério expansionista, há o critério reducionista, que pugna o entendimento de que os dados pessoais são aqueles que identificam imediatamente a pessoa natural.

> Art. 5º Para os fins desta Lei, considera-se:
>
> [...]
>
> II - dado pessoal sensível: 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;

Esse conceito também não é novo no ordenamento jurídico brasileiro. O artigo 3º, parágrafo 3º, inciso II, da Lei n. 12.414/2011[16] faz alusão às informações consideradas sensíveis, que são aquelas relativas à origem social e étnica, à saúde, à informação genética, à orientação sexual e às convicções políticas, religiosas e filosóficas.

Em razão da natureza dos dados pessoais sensíveis, a Lei 12.414/2011 oferta proteção extraordinária, sobretudo porque sua utilização inadequada pode conduzir a situações discriminatórias ou permitir que haja identificação de forma inequívoca e persistente[17]. Esses dados, conforme previsto no inciso II do artigo 3º supracitado, referem-se à origem racial ou étnica, à convicção religiosa, à opinião política ou a dados relativos à saúde ou à vida sexual, dados genéticos ou biométricos, quando estiverem vinculados a uma pessoa natural.

Assim:

> Quando se pensa em dados que exprimem a orientação sexual, religiosa, política, racial, estado de saúde ou filiação sindical, surge a preocupação em haver distinção ou diferenciação de uma pessoa por conta de tais aspectos da sua personalidade[18].

Aqui é importante entender que o inciso II do artigo 3º da Lei n. 12.414/2011 deve ser interpretado junto com o conceito de dado pessoal previsto no seu inciso I, especificamente no que se refere à aptidão do dado ou informação em identificar uma pessoa natural ou torná-la identificável.

Feigelson e Siqueira afirmam que os dados sensíveis podem ser classificados em quatro categorias: (i) dados pessoais sensíveis quanto à origem; (ii) dados pessoais sensíveis de crenças; (iii) dados pessoais sensíveis sexuais; e (iv) dados pessoais sensíveis corporais[19]. Os dados relativos à saúde enquadram-se neste último caso.

---

[16] BRASIL. *Lei n. 12.414, de 09 de junho de 2011.* Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm. Acesso em: 16 nov. 2021.

[17] FEIGELSON, Bruno; SIQUEIRA, Antonio Henrique Albani (Coords.). *Comentários à Lei Geral de Proteção de Dados:* Lei 13.709/2018. São Paulo: Editora Revista dos Tribunais, 2019. p. 92.

[18] BIONI, Bruno Ricardo. *Proteção de dados pessoais:* a função e os limites do consentimento. Rio de Janeiro: Forense, 2019. p. 118.

[19] FEIGELSON, Bruno; SIQUEIRA, Antonio Henrique Albani (Coords.). *op. cit.,* p. 92.

Os dados sensíveis são uma espécie de dados pessoais[20], revelando, porém, uma situação de vulnerabilidade especial em decorrência do conteúdo carregado por essa categoria de dados. Assim, a natureza sensível desses dados reside no fato de que sua utilização descontrolada pode ocasionar prejuízos a direitos fundamentais das pessoas, especialmente os ligados à privacidade, intimidade, igualdade e dignidade da pessoa humana.

Segundo Bioni, um determinado dado trivial pode se transformar em um dado sensível, sobretudo em razão das ferramentas existentes para tratamento de dados, permitindo a correlação de dados com um objetivo preditivo[21]. Por exemplo: em 2012, foi revelado que a loja de departamentos Target conseguiu descobrir se suas clientes estavam grávidas antes mesmo de comprarem as primeiras fraldas para seus bebês. Isso foi possível em razão de uma análise do histórico das compras efetuadas pelas clientes, tais como nome, e-mail e outros dados demográficos vinculados ao número do cartão de crédito. Padrões de comportamento foram descobertos após a análise de dados triviais, permitindo com que a Target iniciasse uma campanha de *marketing* em que cupons de desconto para produtos ligados à gravidez eram enviados às mulheres. "É possível, portanto, identificar individualidades mais sensíveis das pessoas, tais como orientação sexual, raça e estado de saúde, a partir de informações triviais"[22], o que demonstra que a utilização de dados sensíveis tem um potencial invasivo na esfera da intimidade e privacidade muito maior do que um dado pessoal comum, além de um potencial de ofensividade à dignidade da pessoa humana muito mais intenso.

Com isso:

> A diferenciação no tratamento de dados pessoais sensíveis em relação aos dados pessoais não sensíveis torna-se destaque na Lei em comento [...] porque há uma preocupação especial no que diz respeito a assegurar a privacidade, assim como assegurar que tais dados não possam ser utilizados contra os titulares, trazendo-lhes restrições ao acesso a bens, serviços e ao exercício de direitos[23].

Nesse cenário, o artigo 11 da LGPD prevê que o tratamento de dados pessoais somente poderá ocorrer em determinadas hipóteses, disciplinadas nos incisos I e II, sendo que qualquer tratamento dessa categoria de dados deve observar as normas previstas no artigo 11 da LGPD: "Aplica-se o disposto neste artigo a qualquer tratamento de dados pessoais que revele dados pessoais sensíveis e que possa causar dano ao titular, ressalvado o disposto em legislação específica".

---

[20] BIONI, Bruno Ricardo. *op. cit.*, p. 118.
[21] *Id. loc. cit.*
[22] *Id. Ibid.,* p. 118-119.
[23] FEIGELSON, Bruno; SIQUEIRA, Antonio Henrique Albani (Coords.). *op. cit.,* p. 93.

As hipóteses permissivas do tratamento podem ser divididas naquelas em que houver o consentimento do titular de dados (inciso I) e naquelas que dispensam o consentimento e que são disciplinadas em sete alíneas do inciso II do artigo 11 da LGPD. A primeira e mais trivial hipótese, prevista no inciso I do artigo 11, diz respeito às situações em que houver consentimento do titular ou responsável, de forma específica ou destacada, para finalidades específicas. Segundo o inciso XII do artigo 5º da LGPD, o consentimento consiste na manifestação livre, informada e inequívoca por meio da qual o titular expressa sua concordância com o tratamento de seus dados pessoais para uma finalidade determinada. Importante salientar que o consentimento é uma das bases legais previstas para o tratamento de dados pessoais. Todavia:

> [...] em razão do alto grau de transparência perante o titular, é a hipótese que pode trazer mais segurança jurídica para o controlador, a quem incumbe o ônus da prova de que foi obtido em conformidade com a lei[24].

A LGPD veda, portanto, o tratamento de dados pessoais sensíveis com esteio em consentimento genérico e sem finalidades adrede estabelecidas.

Já o inciso II disciplina as hipóteses em que o consentimento não é necessário pelo fato de o tratamento de dados pessoais sensíveis ser **indispensável** – o que significa que, em situações nas quais o tratamento de dados pessoais sensíveis não for absolutamente necessário, sua manipulação estará vedada pela lei. Esse entendimento tem esteio nos princípios da máxima efetividade e da interpretação *pro homine* dos direitos fundamentais e que, diante da utilização do termo "indispensável" pelo legislador, impõe o dever de prestigiar uma hermenêutica que dê a maior efetividade possível ao direito fundamental à proteção de dados pessoais.

Logo, naquelas situações concretas em que o tratamento de dados pessoais sensíveis não for indispensável – mesmo que reflita, em um primeiro momento, qualquer das hipóteses presentes nas alíneas do inciso II do artigo 11 da LGPD –, estarão vedadas ao controlador sua coleta e sua manipulação.

A primeira situação se dá nos casos de cumprimento de obrigação legal ou regulatória pelo controlador, que, neste caso, passa, necessariamente, pelo tratamento de dados pessoais sensíveis, havendo, contudo, o dever de informar o titular acerca desse tratamento[25]. Segundo Maldonado e Blum:

---

[24] MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (Coords). *LGPD:* Lei Geral de Proteção de Dados comentada. 2. ed. São Paulo: Editora Revista dos Tribunais, 2019. p. 117.
[25] FEIGELSON, Bruno; SIQUEIRA, Antonio Henrique Albani (Coords.). *op. cit.,* p. 95.

> [...] nas situações em que se entender que determinados dados pessoais poderão servir como elemento para exercício de direitos em demandas em geral, eles poderão ser armazenados, desde que para essa única e exclusiva finalidade, enquanto subsistir tal necessidade[26].

A situação disciplinada na letra *b* do inciso II do artigo 11 da LGPD diz respeito ao compartilhamento de dados necessário à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos. Envolve, portanto, casos em que a supremacia do interesse público se faz presente, não podendo a execução de políticas públicas ficar à mercê do consentimento de um particular. Também nessas situações, o titular tem o direito de ser informado com respeito a realização de tratamento de seus dados.

Já a alínea *c* dispõe que o tratamento de dados sensíveis também poderá ser realizado sem consentimento do titular quando da realização de estudos por órgãos de pesquisa, prevendo a garantia, sempre que for possível, da anonimização dos dados pessoais sensíveis.

Outra situação de dispensa do consentimento é disciplinada na letra *d* e diz respeito ao exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral.

Os casos que envolverem a proteção da vida ou da incolumidade física do titular ou de terceiro também dispensam o consentimento, situação disciplinada na alínea *e*.

A letra *f* trata dos casos envolvendo a tutela da saúde, exclusivamente nos procedimentos que forem realizados pelos profissionais da área da saúde, serviços de saúde ou por entidades sanitárias, situações que igualmente dispensam o consentimento. A Lei n. 13.853/2019 trouxe alteração na redação original, incluindo o vocábulo "exclusivamente" e a expressão "serviços de saúde".Com isso, fica clara a intenção do legislador de prever uma situação que excepciona a dispensa do consentimento somente naqueles procedimentos realizados por profissionais e órgãos de saúde legalmente autorizados. Ademais, os procedimentos meramente estéticos, mesmo que realizados por profissionais da área de saúde, não são abrangidos pela exceção prevista na alínea *f* do inciso II do artigo 11 da LGPD.

Por fim, a letra *g* do inciso em questão traz a dispensa do consentimento com vistas à garantia da prevenção de fraude e da segurança do titular nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, devendo ser resguardados os direitos mencionados no artigo 9º da LGPD, exceto em caso de

[26] MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (Coords). *LGPD:* Lei Geral de Proteção de Dados comentada, *cit.*,p. 184.

prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

II. A LGPD e os dados referentes à saúde

1. Do compartilhamento de dados sensíveis referentes à saúde na LGPD

Embora o Brasil já contasse com leis esparsas, além de diversos atos normativos e decisões judiciais[27]expressando tutela a pontos relacionados à privacidade e, portanto, aplicáveis aos dados pessoais, foi com a LGPD que o dado pessoal passou a merecer uma proteção específica no ordenamento jurídico pátrio.

Consideradas dados pessoais sensíveis, as informações relativas à saúde têm tratamento específico na LGPD em razão do relevante interesse público envolvido. Logo, a LGPD deixa patente que a tutela da saúde poderá ser considerada como base legal para o tratamento de dados pessoais[28].Importante salientar que dados referentes à saúde podem ser manipulados de duas formas. A primeira diz respeito à utilização de dados sensíveis para fins de estudos em saúde pública, conforme base legal prevista no artigo 11, letra *c* da LGPD. A outra forma de manipulação de dados refere-se ao permissivo da alínea *f* do artigo 11 da LGPD, que diz respeito aos casos envolvendo a tutela da saúde.

Foi visto que a LGPD considera como sensíveis os dados pessoais relativos à saúde (art. 5º, II). Logo, o tratamento desses dados, seja para fins de estudos de saúde pública, seja para a tutela de saúde, deve observar as exigências da LGPD relativas à manipulação de dados considerados sensíveis.

Uma norma aplicável aos dois casos de tratamento de dados relativos à saúde encontra-se disciplinado no parágrafo 4º do artigo 11 da LGPD:

> § 4º É vedada a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica, exceto nas hipóteses relativas a prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde, desde que observado o § 5º deste artigo, incluídos os serviços auxiliares de diagnose e terapia, em benefício dos interesses dos titulares de dados, e para permitir:

---

[27] Cite-se como exemplo: SUPERIOR TRIBUNAL DE JUSTIÇA – STJ. Recurso Especial 1.419.697/RS, Segunda Seção, Relator Paulo de Tarso Sanseverino, Julgamento: 12/11/2014. Disponível em: https://bdjur.stj.jus.br/jspui/bitstream/2011/114173/REsp1419697.pdf. Acesso em: 16 nov. 2021; e, mais recentemente: SUPERIOR TRIBUNAL DE JUSTIÇA – STJ. Recurso Especial 1.758.799/MG, Terceira Turma, Relator Nancy Andrighi, Julgamento: 12/11/2019. Disponível em: https://processo.stj.jus.br/processo/revista/documento/mediado/?componente=ITA&sequencial=1888267&num_registro=201700065219&data=20191119&formato=PDF. Acesso em: 16 nov. 2021.

[28] MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (Coords). *LGPD:* Lei Geral de Proteção de Dados comentada, *cit.,* p. 185.

> I - a portabilidade de dados quando solicitada pelo titular; ou
>
> II - as transações financeiras e administrativas resultantes do uso e da prestação dos serviços de que trata este parágrafo.

Da leitura do dispositivo acima, é fácil notar que a regra é a vedação da comunicação e do uso compartilhado entre controladores de dados pessoais sensíveis que sejam relacionados à saúde quando há o desiderato de obtenção de vantagem econômica.

> Em regra geral, dados de saúde não poderão ser compartilhados entre controladores, caso haja o objetivo de vantagem econômica, conceito que deve ser entendido de forma ampla, contemplando vantagens diretas ou indiretas, inclusive aquelas de caráter não estritamente monetário[29].

Como pode haver confusão quando é feita a leitura dos parágrafos 3º e 4º do artigo 11 da LGPD, é importante destacar que o parágrafo 3º disciplina a possibilidade de comunicação ou uso compartilhado de dados pessoais sensíveis entre controladores com a finalidade de obtenção de lucro, asseverando que poderá haver vedação ou regulamentação pela Autoridade Nacional de Proteção de Dados (ANPD), ouvidos órgãos setoriais do poder público. Isso significa que a regra prevista no parágrafo em questão é a permissão da comunicação e do compartilhamento para fins de lucro, havendo a necessidade, porém, de consentimento do titular[30]. Em outras palavras, a norma prevista no parágrafo 3º permite a comunicação e o compartilhamento com a finalidade de lucro de qualquer dado pessoal sensível, desde que haja o consentimento do titular e que o dado sensível não seja relativo à saúde, na medida em que para este há vedação específica no parágrafo 4º do artigo 11 da LGPD.

Embora o parágrafo 3º possa incidir sobre situações que envolvam dados sensíveis relativos à saúde e em que haja o consentimento do titular, ele possibilita que a ANPD vede ou regulamente a comunicação ou o uso compartilhado com fins econômicos, mesmo quando houver esse consentimento do titular. Logo:

> Uma vez que já existe vedação de compartilhamento de dados sensíveis pelo controlador para fins econômicos sem o devido consentimento do titular, pode-se concluir que o § 3º possibilita que a autoridade nacional vede ou faça restrições para tal possibilidade, mesmo em casos de consentimento pelo titular[31].

A situação prevista no parágrafo 4º do artigo 11 da LGPD é específica aos dados sensíveis relativos à saúde. Assim, "o § 4º surge diante da preocupação do

[29] MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (Coords). *LGPD*: Lei Geral de Proteção de Dados comentada, *cit.*, p. 201.
[30] FEIGELSON, Bruno; SIQUEIRA, Antonio Henrique Albani (Coords.). *op. cit.,* p. 99.
[31] *Id. Ibid.*, p. 99.

legislador no sentido de resguardar o particular, no tocante ao eventual uso de dados no bojo de políticas comerciais relativas ao setor da saúde"[32].

Como já destacado, a leitura do parágrafo 4º do artigo 11 da LGPD requer sua interpretação em conjunto com o parágrafo 3º do mesmo artigo. Isso porque o parágrafo 3º traz uma previsão geral que incide sobre as situações disciplinadas nos incisos I e II do parágrafo4º. Assim, é possível à ANPD vedar ou regulamentar as situações previstas nos incisos I e II do parágrafo 4º com fundamento no parágrafo 3º do artigo 11 da LGPD. Desta maneira, a vedação prevista no parágrafo 4º em comento traz exceções, a saber, nas hipóteses relativas à prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde, devendo estas exceções observarem o que prescreve o parágrafo 5º do artigo 11 da LGPD.

Ademais, o parágrafo 4º do artigo 11 da LGPD prevê que devem ser incluídos nessa exceção os serviços auxiliares de diagnose e terapia em benefício dos interesses dos titulares de dados e, também, para que se permitam a portabilidade de dados quando requerida pelo titular e a realização das transações financeiras e administrativas que resultarem do uso e da prestação dos serviços de que trata o parágrafo 4º.

Por fim, o parágrafo 5º do artigo 11 da LGPD veda às operadoras de planos privados de assistência à saúde a realização de tratamento de dados de saúde objetivando a seleção de riscos na contratação de qualquer modalidade, bem como na contratação e exclusão de beneficiários.

2. Tratamento de dados sensíveis com fundamento no artigo 11, inciso II, alínea *f* da LGPD

O permissivo para tratamento de dados sensíveis com vistas à tutela da saúde vem disciplinado no inciso II, alínea *f* do artigo 11 da LGPD:

> Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:
>
> [...]
>
> II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:
>
> [...]
>
> f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária.

[32] *Id. Ibid.*, p. 100.

Trata-se de permissivo que dispensa o fornecimento de consentimento pelo titular, dados o bem tutelado (a saúde) e sua importância. Por outro lado, o setor de saúde possui características peculiares que demandam uma disciplina específica com relação ao tratamento de dados pessoais sensíveis, dispensando o consentimento do titular.

Primeiramente, deve ser destacado que a letra *f* do inciso II do artigo 11 da LGPD prevê que a dispensa do consentimento do titular ocorrerá nas hipóteses em que ela for **indispensável** para a situação disciplinada. Portanto, não é qualquer situação que autoriza o uso de dados pessoais sensíveis sem o consentimento para a tutela da saúde, mas somente aqueles casos em que o procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária dependam do tratamento de dados pessoais sensíveis. A possibilidade de tratamento de dado pessoal sensível deverá ser avaliada em cada caso concreto, não sendo possível estabelecer padrões prévios nos quais a manipulação dos dados sensíveis poderá ser feita sem o consentimento, o que exige do profissional de saúde cautela para não praticar conduta em desconformidade com a LGPD.

Outro ponto do dispositivo em questão refere-se à expressão "tutela da saúde". O termo "tutela" provém do latim *tueri*, cujo significado é proteger. E, sob o ponto de vista jurídico, a tutela implica a proteção ofertada pela lei a algum bem da vida. No caso da LGPD, o termo "tutela" deve ser interpretado de uma maneira mais ampla, para além dos limites do sistema jurídico e com entendimento que englobe todo e qualquer procedimento realizado por profissionais da área da saúde, serviços de saúde ou autoridade sanitária que redunde na proteção à saúde.

É preciso levar em conta que a Constituição Federal de 1988 eleva a saúde à categoria de direito fundamental, ligado à ideia de:

> [...] dignidade da pessoa humana e o direito à vida, sendo a Declaração Universal de Direitos Humanos de 1948 categórica em afirmar que toda pessoa tem direito a um padrão de vida que permita assegurar a si e à sua família saúde e bem-estar[33].

A importância do bem tutelado foi considerada pela LGPD, tornando dispensável o consentimento nos casos em que a proteção à saúde depender do tratamento de dados sensíveis relacionados à saúde. Não significa uma mitigação da proteção dos dados pessoais sensíveis pela LGPD, mas uma harmonização dessa proteção com o direito fundamental à saúde. Ou seja,"[...] a tutela da saúde justifica o tratamento de dados pessoais na medida em que preserva um aspecto essencial

[33] BOTELHO, Marcos César. Gestão discursiva da saúde. *Revista Direito e Liberdade*, Esmarn, Natal, v. 17, n. 3, p. 166, 2015. Disponível em: http://ww2.esmarn.tjrn.jus.br/revistas/index.php/revista_direito_e_liberdade/article/download/932/670.

da vida humana"[34]. Logo, é possível o tratamento de dados sensíveis independentemente de consentimento do titular por operadoras, gestores do SUS e serviços de saúde, abrangendo os serviços de saúde de uma forma ampla.

Outra questão importante é a utilização do termo "exclusivamente" pelo legislador. Isso significa que a dispensa do consentimento nos casos indispensáveis à tutela da saúde se dará tão somente naqueles procedimentos realizados por profissionais de saúde, serviços de saúde ou autoridade sanitária.

Há uma disciplina restritiva na letra *f* do inciso II do artigo 11 da LGPD que possibilita que os profissionais de saúde, os serviços de saúde ou a autoridade sanitária se valham do permissivo. Assim:

> Por profissionais de saúde entendemos aquelas pessoas naturais formadas em algum ramo da ciência que seja relacionado com a vida, saúde ou doença humana, tais como: medicina, enfermagem, fonoaudiologia, análises clínicas, fisioterapia, educação física, odontologia, psicologia, terapia ocupacional, farmácia, biologia, entre outras[35].

Os serviços de saúde consistem nos estabelecimentos que são destinados à promoção da saúde do indivíduo, visando a protegê-lo de toda a sorte de doenças e agravos, além de prevenirem e limitarem eventuais danos que possam ser causados à pessoa, objetivando a reabilitação de sua capacidade física, psíquica e social quando afetada[36].

Há que se destacar que a redação original não fazia alusão aos serviços de saúde, havendo a consequente exclusão da permissão de tratamento de dados pessoais sensíveis ligados à saúde pelas entidades privadas[37]. Todavia, a Lei n.13.853/2019 deu nova redação ao inciso VIII do artigo 7º e à alínea *f* do inciso II do artigo 11 da LGPD, incluindo os serviços de saúde e harmonizando-os com a disciplina constitucional que permite a atuação privada na saúde. Lembram Dallari e Nunes Júnior que, no que tange à participação da iniciativa privada fora do SUS, "[...] não houve restrições, o que revela a possibilidade dos entes privados prestarem assistência à saúde nos distintos níveis de complexidade"[38].

Desta forma, permitir que profissionais de saúde e entidades sanitárias utilizassem dados sensíveis para a tutela da saúde, mas vedar os serviços de saúde de fazer o mesmo, consistia em uma falha no texto da LGPD que foi corrigida pela Lei n. 13.853/2019.

---

[34] COTS, Márcio; OLIVEIRA, Ricardo. *op. cit.,* p. 85.
[35] *Id. loc. cit.*
[36] AGÊNCIA NACIONAL DE VIGILÂNCIA SANITÁRIA - ANVISA. *Tecnologia da Organização dos Serviços de Saúde*. Disponível em: http://www.anvisa.gov.br/servicosaude/organiza/index.htm. Acesso em: 21 fev. 2020.
[37] COTS, Márcio; OLIVEIRA, Ricardo. *op. cit.,* p. 86.
[38] DALLARI, Sueli Gandolfi; NUNES JÚNIOR, Vidal Serrano. *Direito sanitário*. São Paulo: Verbatim, 2010. p. 97.

Já as entidades sanitárias são definidas pela Portaria n. 1.139/2013, do Ministro da Saúde[39], cujo artigo 4º, inciso III prescreve: "[...]III - autoridade sanitária: órgão ou agente público competente da área da saúde, com atribuição legal no âmbito da vigilância e da atenção à saúde". Ou seja, as autoridades sanitárias são os "[...] entes de direito público da administração direta ou indireta dedicada a algum aspecto da preservação da saúde pública"[40].

3. Tratamento de dados pessoais para fins de estudos em saúde pública

A LGPD também traz norma específica quanto ao tratamento de dados pessoais para fins de estudos em saúde pública. A disciplina consta do artigo 13, cujo *caput* prescreve:

> Art. 13. Na realização de estudos em saúde pública, os órgãos de pesquisa poderão ter acesso a bases de dados pessoais, que serão tratados exclusivamente dentro do órgão e estritamente para a finalidade de realização de estudos e pesquisas e mantidos em ambiente controlado e seguro, conforme práticas de segurança previstas em regulamento específico e que incluam, sempre que possível, a anonimização ou pseudonimização dos dados, bem como considerem os devidos padrões éticos relacionados a estudos e pesquisas.

De acordo com o dispositivo em tela, os órgãos de pesquisa terão acesso franqueado a bases de dados pessoais para fins de estudos em saúde pública, mas esse acesso somente é franqueado quando estiver envolvido estudo em saúde pública, sendo este o requisito (e não o fato de se tratar de um órgão de pesquisa). Assim: "[...] deve ser esclarecido que os conceitos trazidos no presente artigo são limitados tão somente para o uso dos dados pessoais para a realização de estudos e pesquisas em saúde pública"[41].

Ademais, para evitar qualquer confusão quanto ao conceito de "órgão de pesquisa", a LGPD traz no artigo 5º, inciso XVIII, uma definição legal, afirmando que órgão pesquisa consiste em órgão ou entidade da administração pública direta ou indireta, bem como pessoa jurídica de direito privado sem fins lucrativos que esteja constituída legalmente sob as leis brasileiras, que possua sede e foro no país e cuja missão institucional ou objetivo social ou estatutário inclua a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico.

Outro ponto importante da lei é a restrição do local onde pode ser feito o tratamento de dados: somente dentro do órgão e para a estrita finalidade de realização de estudos e pesquisas. Dúvida poderia surgir em casos em que a pesquisa

[39] MINISTÉRIO DA SAÚDE. *Portaria n. 1.139, de 10 de junho de 2013.* Disponível em: http://bvsms.saude.gov.br/bvs/saudelegis/gm/2013/prt1139_10_06_2013.html. Acesso em: 24 fev. 2020.
[40] COTS, Márcio; OLIVEIRA, Ricardo. *op. cit.,* p. 85.
[41] MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (Coords). *LGPD:* Lei Geral de Proteção de Dados comentada, *cit.,* p. 206.

demande coleta de dados em campo – que, de acordo com a LGPD, não poderia ser realizada, pois implicaria tratamento de dados pessoais fora da organização. Uma leitura do *caput* do artigo 13 da LGPD aponta, à primeira vista, que os órgãos de pesquisa poderão ter "acesso a bases de dados pessoais", o que remete à ideia de acesso a bases de dados consolidadas – uma base de dados consiste na "consolidação de todos os dados tidos como operáveis sob qualquer forma e armazenamento em qualquer local"[42]. Entende-se que uma possível interpretação da restrição do *caput* do artigo 13 da LGPD seria considerar a expressão "dentro do órgão" como o tratamento que fosse realizado dentro da estrutura organizacional do órgão e sob sua supervisão; essa interpretação teria fundamento no artigo 2º da LGPD, especialmente no inciso V, que estabelece que a disciplina da proteção de dados deverá ter como fundamentos o desenvolvimento econômico e tecnológico e a inovação, que não se coadunam com uma restrição da pesquisa a um lugar geográfico, impedindo situações nas quais pesquisas de campo para coleta de dados e informações forem imprescindíveis.

A referência do *caput* do artigo 13 à estrita finalidade de realização de estudos e pesquisas se coaduna com o princípio da finalidade positivada no inciso I do artigo 6º da LGPD, que exige que as atividades de tratamento de dados deverão observar o princípio da finalidade, ou seja, o tratamento realizado com fins legítimos, específicos, explícitos e informados ao titular, vedando-se a possibilidade de tratamento posterior em desconformidade com essas finalidades. Assim:

> O princípio da finalidade conta com grande relevância prática, pois, por meio dele, é garantido ao titular, mediante informação prévia, as fronteiras da legalidade do tratamento de seus dados, delimitando os propósitos do tratamento, desde que lícitos, e de terceiros que poderão ou não ter acesso aos dados[43].

O franqueamento à base de dados pessoais somente é possível se observada a finalidade de realização de estudos e pesquisas. Se inexistir qualquer estudo ou pesquisa ou se, no decorrer de sua execução, houver desvirtuamento da finalidade, ausente estará a base legal para o tratamento de dados pessoais sensíveis, impondo-se o imediato cessamento do tratamento sob pena de afronta à LGPD, com a responsabilização do controlador ou operador.

O artigo 13 exige, ainda, que os dados pessoais sejam mantidos em ambiente controlado e seguro, em conformidade com as práticas de segurança previstas em regulamento específico. Aqui, além de regulamentos específicos editados pela Autoridade Nacional de Proteção de Dados, práticas de segurança previstas em normativos

[42] SAWAYA, Márcia Regina. *Dicionário de informática & internet inglês/português*. São Paulo: Nobel, 1999. p. 112.
[43] MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (Coords). *LGPD:* Lei Geral de Proteção de Dados comentada, *cit.*, p. 138.

setoriais devem ser levadas em consideração, podendo ser citadas como exemplo as normas ABNT NBR ISO/IEC 27.001 e ABNT NBR ISO/IEC 27.002.

Há, ainda, a exigência, sempre que possível, de anonimização ou pseudonimização dos dados. O conceito de anonimização é dado no inciso XI do artigo 5º da LGPD: trata-se da utilização de meios técnicos razoáveis e disponíveis no momento do tratamento que resultem na eliminação da associação, direta ou indireta, do dado a uma pessoa natural. O resultado é o dado anonimizado, que o inciso III do artigo 5º da LGPD define como aquele relativo a um determinado titular que não possa ser identificado.

Já o conceito jurídico de pseudonimização vem previsto no parágrafo 4º do artigo 13 da LGPD e diz respeito ao tratamento por meio do qual um dado perde sua possibilidade de associação, direta ou indireta, a um indivíduo, a não ser pela utilização de informação adicional que esteja mantida separada pelo controlador em ambiente controlado e seguro. O conceito de pseudonimização restringe a situação prevista no *caput* do artigo 13 da LGPD, ao contrário do Regulamento Geral sobre a Proteção de Dados na Europa, que adotou um conceito mais amplo[44]. Saliente-se que:

> [...] a pseudonimização é pela primeira vez mencionada na lei brasileira no § 4º do art. 13, isso porque o legislador considerou que pesquisas nas áreas de saúde pública são tão relevantes que permitem duas técnicas distintas (anonimização e pseudonimização)[45].

Por fim, padrões éticos devem ser observados em estudos e pesquisas, podendo ser citada como exemplo a Resolução n. 466/2012[46], do Conselho Nacional de Saúde e que disciplina as pesquisas realizadas envolvendo seres humanos. A LGPD também abrange padrões éticas, exigindo que a divulgação dos resultados ou de qualquer excerto do estudo ou da pesquisa a que se refere o *caput* do artigo 13, em hipótese alguma, revele dados pessoais. Isso significa que, para a divulgação dos resultados ou mesmo de excertos do estudo, deverá haver, no mínimo, a pseudonimização dos dados, pois a exigência do parágrafo 1º do artigo 13 é de que não poderá haver a revelação de dados pessoais em hipótese alguma. Segundo Maldonado e Blum:

> Neste parágrafo entendemos que há clara referência ao fato de que a divulgação de resultados e de trechos do estudo somente deve ocorrer, mediante, no mínimo, realização de prévia pseudonimização dos dados, a qual é obrigatória[47].

---

[44] MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (Coords). LGPD: Lei Geral de Proteção de Dados comentada, *cit*., p. 207.

[45] FEIGELSON, Bruno; SIQUEIRA, Antonio Henrique Albani (Coords.). *op. cit.,* p. 106.

[46] CONSELHO NACIONAL DE SAÚDE – CNS. *Resolução n. 466, de 12 de dezembro de 2012*. Disponível em: https://bvsms.saude.gov.br/bvs/saudelegis/cns/2013/res0466_12_12_2012.html. Acesso em: 16 nov. 2021.

[47] MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (Coords). *LGPD:* Lei Geral de Proteção de Dados comentada, *cit.,* p. 206.

Contudo, embora o artigo 13 da LGPD permita a utilização de técnicas de anonimização ou pseudonimização, entende-se que a escolha pelo controlador não é discricionária. O que determina qual das técnicas poderá ser empregada é a garantia de sua efetividade, ou seja, aquela que tornará o processo seguro. Desta maneira, diante do caso concreto, o controlador deverá avaliar se o emprego de métodos de pseudonimização serão suficientes para garantir a segurança do tratamento dos dados, com a diminuição do risco de divulgação indevida desses dados. Caso contrário, deverá obrigatoriamente implementar medidas de anonimização.

O parágrafo 2º do artigo 13 da LGPD prevê que a responsabilidade pela segurança da informação a que se refere o *caput* será do órgão de pesquisa, vedando de forma absoluta a transferência dos dados a terceiro. O dispositivo, ainda, deixa clara a responsabilidade do órgão de pesquisa no que tange à implementação das medidas jurídicas e técnicas objetivando a segurança da informação.

Há que se destacar que o artigo 13 da LGPD depende de regulamentação pela Autoridade Nacional de Proteção de Dados, conforme se depreende da leitura de seu parágrafo 3º. A leitura do dispositivo também indica que a ANPD deverá consultar as autoridades de saúde e sanitárias visando a estabelecer conjuntamente parâmetros de acesso pelos órgãos de pesquisa a bases de dados pessoais. Como visto, a ANPD é definida no artigo 5º, inciso XIX, enquanto a autoridade sanitária tem sua definição apresentada na Portaria n. 1.139/2013 do Ministro da Saúde.

Considerações finais

A LGPD dá uma nova dimensão para o tratamento de dados no Brasil ao disciplinar a proteção de dados pessoais enquanto um direito fundamental. Com isso, o Brasil entra para o grupo de países que dispõe sobre normas de proteção aos dados pessoais, o que certamente terá impacto positivo no âmbito das relações comerciais.

Na esteira das nações desenvolvidas, a LGPD reconhece a existência de dados pessoais considerados sensíveis, a saber, aqueles que se referem a origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, bem como dados referentes à saúde ou à vida sexual e dados genéticos ou biométricos, quando vinculados a uma pessoa natural.

Nesse contexto, foi visto que dados relativos à saúde são considerados sensíveis, merecendo um tratamento específico pela LGPD dada a importância dessa categoria de dados. Há uma disciplina relativa ao uso de dados sensíveis relacionados à saúde na alínea *f*, inciso II, do artigo 11 da LGPD, na hipótese de o tratamento dispensar o consentimento quando for indispensável para a tutela da saúde, em procedimento levado a cabo por profissionais da área da saúde, serviços de saúde ou autoridade sanitária.

Com um viés voltado ao interesse público relevante no tratamento de dados pessoais sensíveis relativos à saúde, a LGPD veda a comunicação ou o uso

compartilhado entre controladores dos dados sensíveis relativos à saúde com o objetivo de obtenção econômica, excepcionados os casos envolvendo a prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde.

Outrossim, houve cuidado na LGPD com relação a utilização de dados pessoais para fins de estudos em saúde pública, havendo uma disciplina específica no artigo 13 que prescreve a possibilidade de uso dessa categoria de dados desde que respeitados requisitos específicos, como o tratamento dentro do órgão e em conformidade com as finalidades específicas, além de prever que os dados não podem ser transferidos a terceiros em hipótese alguma e exigir, no mínimo, a pseudonimização dos dados quando da publicação de resultados de pesquisa.

Com a entrada em vigor da LGPD, profissionais da saúde, clínicas médicas, hospitais e centros de saúde, entre outros, que realizarem tratamento de dados pessoais sensíveis relacionados à saúde deverão adotar medidas para adaptar suas atividades às normas previstas na LGPD, sob pena de estarem em desconformidade e sujeitos às sanções previstas na norma, que podem ir desde a aplicação de multas pecuniárias até a proibição do uso de dados pessoais sensíveis.

Referências

AGÊNCIA NACIONAL DE VIGILÂNCIA SANITÁRIA - ANVISA. *Tecnologia da Organização dos Serviços de Saúde*. Disponível em: http://www.anvisa.gov.br/servicosaude/organiza/index.htm. Acesso em: 21 fev. 2020.

AMARAL, Fernando. *Introdução à ciência de dados*. Rio de Janeiro: Alta Books, 2016.

BIONI, Bruno Ricardo. *Proteção de dados pessoais*: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019.

BOTELHO, Marcos César. Gestão discursiva da saúde. *Revista Direito e Liberdade*, Esmarn, Natal, v. 17, n. 3, p. 159-182, 2015. Disponível em: http://ww2.esmarn.tjrn.jus.br/revistas/index.php/revista_direito_e_liberdade/article/download/932/670.

COTS, Márcio; OLIVEIRA, Ricardo. *Lei Geral de Proteção de Dados Pessoais comentada*. 2. ed. São Paulo: Editora Revista dos Tribunais, 2019.

DALLARI, Sueli Gandolfi; NUNES JÚNIOR, Vidal Serrano. *Direito sanitário*. São Paulo: Verbatim, 2010.

FEIGELSON, Bruno; SIQUEIRA, Antonio Henrique Albani (Coords.). *Comentários à Lei Geral de Proteção de Dados:* Lei 13.709/2018. São Paulo: Editora Revista dos Tribunais, 2019.

FRANCO, Paulo Alves. *Lei Geral de Proteção de Dados Pessoais comentada*. Leme-SP: Imperium, 2020.

GOLDSCHMIDT, Ronaldo; PASSOS, Emmanuel; BEZERRA, Eduardo. *Data mining:* conceitos, técnicas, algoritmos, orientações e aplicações. 2. ed. Rio de Janeiro: Elsevier, 2015.

HINTZBERGEN, Jule *et al*. *Fundamentos de segurança da informação*: com base na ISSO 27001 e na ISSO 27002. Rio de Janeiro: Brasport, 2018.

MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (Coords). *Comentários ao GDPR:* Regulamento Geral de Proteção de Dados da União Europeia. São Paulo: Editora Revista dos Tribunais, 2018.

MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (coords). *LGPD:* Lei Geral de Proteção de Dados comentada. 2. ed. São Paulo: Editora Revista dos Tribunais, 2019.

MAYER-SCHÖNBERGER, Viktor; CUKIER, Kenneth. *Big data:* como extrair volume, variedade, velocidade e valor da avalanche de informação cotidiana. Rio de Janeiro: Elsevier, 2013.

O'BRIEN, James A.; MARAKAS, George M. *Administração de sistemas de informação*. 15. ed. Porto Alegre: AMGH, 2013.

SAWAYA, Márcia Regina. *Dicionário de informática & internet inglês/português.* São Paulo: Nobel, 1999.

SCHUTT, Rachel; O'NEIL, Cathy. *Doing data science*. Sebastopol: O'Reilly Media, 2014.

STAIR, Ralph M.; REYNOLDS, George W. *Princípios de sistemas de informação*. Tradução da 6. ed. americana. São Paulo: Pioneira Thomson Learning, 2006.

Marcos César Botelho – Doutorado em Direito Constitucional pela Instituição Toledo de Ensino (ITE); mestrado em Direito Constitucional pelo Instituto Brasiliense de Direito Público (IDP). Professor adjunto do Programa de Mestrado em Ciências Jurídicas na Universidade Estadual do Norte do Paraná (UENP). Analista de Sistemas. Jacarezinho/PR, Brasil. *E-mail*: marcos.botelho@uenp.edu.br

Elimei Paleari do Amaral Camargo – Doutorado em Educação pela Universidade Metodista de Piracicaba (Unimep); mestrado em Direito pela Universidade de Ribeirão Preto (Unaerp); graduação em Direito pela Instituição Toledo de Ensino (ITE/Bauru). Professora adjunta da Universidade Federal de Rondônia (UNIR). Cacoal/RO, Brasil. *E-mail*: elimei@unir.br