Revista Jurídica vol. 03, n°. 70, Curitiba, 2022. pp. 01 - 23

A PROTEÇÃO JURÍDICA DOS DADOS PESSOAIS SENSÍVEIS RELATIVOS À SAÚDE

JURIDICAL PROTECTION OF SENSITIVE PERSONAL DATA RELATED TO HEALTH CONCERNS

ZULMAR FACHIN

Doutor em Direito Constitucional (UFPR). Mestre em Ciência Política e Direito (UEL). Licenciado em Letras. Professor na UEL e no Programa de Doutorado e Mestrado em Ciência Jurídica na Universidade - Unicesumar. Coordenador do Mestrado da Escola de Direito das Faculdades Londrina. Membro eleito da Academia Paranaense de Letras Jurídicas. Presidente do IDCC E-mail: zulmarfachin@uol.com.br

ANABELA CRISTINA HIRATA

Mestranda no Programa de Mestrado Profissional em Direito, Sociedade e Tecnologias da Escola de Direito das Faculdades Londrina. Aluna Especial na disciplina “Inteligência Artificial e a Jurisprudência do Futuro” no Programa de Mestrado da Faculdade de Direito da USP. Bacharel em Direito pela Pontifícia PUC - PR. E-mail: anabelahirata@hotmail.com

RESUMO

Objetivo: O texto é uma reflexão sobre a proteção dos dados pessoais sensíveis na Lei Geral de Proteção de Dados Pessoais (LGPD). Tem por objetivo analisar a forma como a saúde, espécie de dado pessoal sensível, é protegida por essa lei. A pesquisa considera que estabelecer a tutela efetiva dos dados pessoais relativos sensíveis à saúde significa proteger uma dimensão dos direitos da personalidade.

Metodologia: Adota o método hipotético-dedutivo, com a utilização de técnicas de pesquisa bibliográfica e documental, mediante a utilização de livros e de artigos científicos impressos e digitais, bem como da legislação específica sobre o tema.

[Received/Recebido: Março 19, 2022; Accepted/Aceito: junho 15, 2022]

Resultados: O trabalho reconhece a existência de proteção legislativa dos dados pessoais sensíveis, mas aponta para a necessidade de haver proteção efetiva deles, especialmente, no que tange à saúde por parte dos agentes de tratamento, empresas, instituições e governos.

Contribuição: O texto poderá servir de ponto inicial para estudos relativos a cada espécie de dado pessoal sensível, especialmente a saúde, previsto na LGPD.

Palavras-chave: Dados Pessoais Sensíveis; Direitos da Personalidade; LGPD; Saúde.

ABSTRACT

Objective: *The paper is a reflection about sensitive personal data in the General Law of Personal Data Protection - GLPDP (Lei Geral de Proteção de Dados Pessoais - LGPD). The research aims to analyze how health, a type of sensitive personal data, is protected by this law. The study considers that stablishes the effective tutelage of sensitive personal data related health concerns means to protect a dimension of personality rights.*

Methodology: *The research adopts the hypothetical-deductive methods based on the usage of techniques from documental and bibliographical research by means of the handling of printed and digital books and scientific articles as well from the specific legislation about the theme.*

Results: *the paper recognizes the existence of the legislative protection of sensitive personal data but points to the necessity of having effectiveness protection of them specially, in what aims to health concerned to treatment agents, companies, institutions and governments.*

Contribution: *This research prospects to serve as initial point to studies relative to each type of sensitive personal data specially, the health presented in the General Law of Personal Data Protection.*

Keywords: *Sensitive personal data; Health; General law of personal data protection; Personality rights.*

1 INTRODUÇÃO

O texto é uma reflexão sobre os dados pessoais sensíveis, especialmente, os relativos à saúde, protegidos pela Lei Geral de Proteção de Dados Pessoais (LGPD).

[Received/Recebido: Março 19, 2022; Accepted/Aceito: junho 15, 2022]

Esse corpo normativo, publicado em 14 de agosto de 2018, trouxe um conjunto de disposições com o propósito de proteger os dados pessoais gerais e os dados pessoais sensíveis.

O objetivo geral da pesquisa é compreender a extensão dos dados pessoais sensíveis protegidos pela LGPD, os quais dizem respeito à ética, à convicção religiosa, à opinião política, à filiação a sindicato ou à organização de caráter religioso, filosófico ou político, bem como os referentes à saúde ou à vida sexual, ao dado genético ou biométrico, quando tais dados estiverem vinculados a uma pessoa natural determinada ou determinável. Já o objetivo específico consiste em analisar a proteção jurídica estabelecida aos dados pessoais sensíveis relativos à saúde.

O tema da pesquisa está delimitado no tempo e no espaço. Sua análise está vinculada às disposições da LGPD, publicadas em 2018, embora faça menção, quando necessário, a outros corpos normativos que, de alguma forma, protegem dados pessoais. Por outro lado, o espaço da pesquisa também está delimitado, visto que trabalha no âmbito do Direito brasileiro, focando, especificamente, na proteção dos dados pessoais sensíveis relativos à saúde, reconhecendo que a saúde é um direito da personalidade.

Para tanto, o problema da pesquisa consiste na seguinte indagação: a LGPD protege adequadamente os dados pessoais sensíveis relativos à saúde? Para responder ao problema da pesquisa, estabelecem-se duas hipóteses de trabalho: os dados pessoais sensíveis relativos à saúde estão protegidos de modo satisfatório na LGPD ou, ao contrário, a proteção dada por essa lei é insatisfatória.

A pesquisa justifica-se devido à elevada importância assumida pelos dados pessoais neste início de século. Reverenciado como o novo petróleo por diversos autores, os dados pessoais, especialmente os de natureza sensível, exigem tratamento eficaz não apenas por parte do legislador, mas também de governos, empresas, instituições e pessoas que realizam seu tratamento. Assim, o não tratamento ou o tratamento inadequado dos dados pessoais sensíveis podem acarretar danos irreparáveis às pessoas que os titularizam.

Se, por um lado, reconhece a evolução da tutela jurídica dos dados pessoais sensíveis, a pesquisa indica, por outro lado, para a necessidade de haver uma

[Received/Recebido: Março 19, 2022; Accepted/Aceito: junho 15, 2022]

proteção efetiva desses dados por parte de governos, empresas, instituições e pessoas que realizam o tratamento.

O trabalho está dividido em três partes. Na primeira, aborda os dados pessoais e os dados pessoais sensíveis, levando em consideração a distinção feita pela própria LGPD. Em seguida, trata da segurança, do sigilo e das boas práticas e de governança de dados pessoais, especialmente, os de natureza sensível, focalizando na saúde. Por fim, analisa a tríplice responsabilidade a que estão submetidos os agentes de tratamento de dados pessoais sensíveis: responsabilidades administrativa, civil e penal.

2 DADOS PESSOAIS E DADOS PESSOAIS SENSÍVEIS: DISTINÇÃO E PROTEÇÃO JURÍDICA

A Lei Geral do Proteção de Dados Pessoais foi publicada em 14 de agosto de 2018. O seu início de vigência, porém, deve ser analisado em momentos distintos. Foi necessário perfazer diversos caminhos e superar várias etapas, até que a totalidade da lei entrasse em vigor. Esse caminho pode ser assim explicitado:

> a) em 14 de agosto de 2018: publicação da Lei 13.709, que instituiu a proteção dos dados pessoais no Brasil. b) em 28 de dezembro de 2018: entrada em vigor do art. 55-A a L, criando a Autoridade Nacional de Proteção de Dados (ANPD); c) em 28 de dezembro de 2018: entrada em vigor dos artigos 58-A e 58-B, disciplinando o Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (CNPD); d) em 18 de setembro de 2020: a própria lei entrou em vigor, mas parcialmente, pois ainda não tiveram vigência os arts. 52 a 54, que tratam das sanções administrativas; e) em 1º de agosto de 20021: entrada em vigor dos arts. 52 a 54, o que implicou no início da vigência completa da lei.

A LGPD, apesar de ser uma lei ordinária (Constituição Federal, art. 47), não pode ser compreendida como uma lei simples ou corriqueira. Além de versar sobre temas muito importantes para as pessoas naturais, empresas, instituições e governos, ela transporta uma vasta experiência humana, projetando-se para o futuro como um verdadeiro monumento jurídico.

[Received/Recebido: Março 19, 2022; Accepted/Aceito: junho 15, 2022]

> Em síntese, a lei arrebata a experiência humana em sua totalidade, do material ao imaterial, do físico ao eletrônico. Protege os titulares de dados pessoais sobre documentos armazenados em nuvens, em servidores, em memória de computadores, ou mesmo em *pendrives*, bem como em fichas físicas, livros de atas, formulários e prontuários em papel, inclusive aqueles guardados nos antigos armários cinzas, que marcaram época em escritórios e repartições (COLOMBO, 2022, p. 3).

Embora o Brasil tenha demorado para adotar uma lei específica de proteção de dados pessoais – quando a LGPD foi publicada, em 2018, mais de uma centena de países já tinham legislado especificamente sobre o tema –, a importância da lei tem sido reconhecida pela doutrina.

> A LGPD não é apenas uma lei de carga normativa. Ela carrega uma série de regras relacionadas à segurança da informação e, com isso, medidas de proteção técnicas e administrativas passam obrigatoriamente a fazer parte do cotidiano dos agentes de tratamento de dados [...]. Trata-se de uma lei de alcance horizontal, exclusivo e homogêneo no que tange à proteção de dados pessoais, o que ilustra simultaneamente sua abrangência de aplicação e sua relevância temática (PALMEIRA, 2022, p. 150).

A LGPD distingue dois tipos de dados, atribuindo a cada um a proteção jurídica necessária. Os dados pessoais consistem na informação relacionada à pessoa natural, seja identificada, seja apenas identificável (art. 5º, inciso I). Já os dados pessoais sensíveis abrangem o "dado pessoal sobre origem racial ou ética, convicção religiosa, opinião política, filiação a sindicato ou à organização de caráter religioso, filosófico ou político", bem como o "dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural" (art. 5, inciso II).

Em face do que estabelece esse dispositivo legal, os dados pessoais sensíveis podem ser classificados em quatro categorias: a) *dados pessoais sensíveis de origem*, referentes à origem racial ou étnica; b) *dados pessoais sensíveis de crenças*, relativos às informações sobre as convicções religiosas, opiniões políticas e a filiação a sindicatos ou a organizações de caráter religioso; c) *dados pessoais sensíveis corporais*, que são dados referentes à saúde, dados genéticos e dados

[Received/Recebido: Março 19, 2022; Accepted/Aceito: junho 15, 2022]

biométricos; d) *dados pessoais sensíveis sexuais*, relativos à vida sexual das pessoas (TEFFÉ, 2022, p. 128).

A doutrina tem advertido que a distinção entre essas duas espécies de dados pessoais não é meramente conceitual, mas tem aptidão para gerar consequências práticas, visto que a própria lei estabeleceu regimes jurídicos diversos. Neste sentido, esclarece Konder:

> A distinção entre dados pessoais em geral e dados pessoais sensíveis não é puramente conceitual, já que a lei prevê disciplina normativa diversa: ao tratamento dos dados pessoais sensíveis se aplicam normas distintas daquelas aplicadas ao tratamento dos dados pessoais não sensíveis, justamente com o objetivo de impedir a utilização desses dados para fins discriminatórios (KONDER, 2020, p. 452).

A LGPD contém diversas normas jurídicas relativas à saúde, categoria de dados pessoais sensíveis, desse modo: a) define a saúde como dado pessoal sensível (art. 5º); b) estabelece as formas de tratamento dos dados pessoais sensíveis (art. 11); c) prevê estudos e pesquisas em saúde pública (art. 13); d) trata da responsabilidade civil do controlador e do operador (art. 42); e) estabelece medidas de segurança e de sigilo (art. 46); f) exige requisitos a serem observados pelos sistemas utilizados para tratamento de dados pessoais sensíveis (art. 49); g) estabelece sanções administrativas aos agentes de tratamento de dados pessoais sensíveis (art. 52).

A saúde é uma categoria de dados pessoais sensíveis. Abrange a saúde individual, a ser usufruída em benefício de cada pessoa e a saúde pública, a qual diz respeito à saúde da população em geral e requer atuação dos governos, os quais devem desenvolver políticas públicas visando ao estabelecimento do bem-estar social.

Os dados sensíveis constituem uma espécie de “núcleo duro” dos dados protegidos pelo Direito e, especialmente, pela LGPD. Além disso, é preciso haver compromisso com a efetivação do direito protegido.

[Received/Recebido: Março 19, 2022; Accepted/Aceito: junho 15, 2022]

> Os dados sensíveis necessitam, mais do que nunca, de uma tutela diferenciada e especial, de forma a se evitar que informações dessa natureza sejam vazadas, usadas indevidamente, comercializadas ou sirvam para embasar preconceitos e discriminações ilícitas em relação ao titular. Todavia, a mera proibição do tratamento de dados sensíveis é inviável, pois, em alguns momentos, o uso de tais dados será legítimo e necessário, além de existirem determinados organismos cuja própria razão de ser estaria comprometida caso não pudessem obter informações desse gênero, como, por exemplo, algumas entidades de caráter político, religioso ou filosófico (VIOLA, 2021, p. 145).

A saúde, assim como a vida sexual, por ser um dado pessoal sensível, necessita receber especial proteção do legislador, das instituições públicas e privadas, bem como das pessoas jurídicas e físicas que tratam de dados pessoais.

Na perspectiva da proteção da privacidade – compreendida não apenas no isolamento, mas também em uma dimensão coletiva –, Rodotá trata do caso específico da saúde, compreendida domo dado pessoal sensível.

> Este é um tema que pode ser examinado com referência a certos dados sensíveis, como os relacionados à saúde. Antes se mencionou que a proteção especial atribuída a esses dados não se justifica somente por se referirem a fatos íntimos, mas também, e às vezes sobretudo, pelo risco que seu conhecimento possa provocar discriminações. Partindo desta consideração, podem ser corretamente enfrentadas algumas questões surgidas em torno da Aids e dos dados relativos às características genéticas de uma pessoa (RODOTÁ, 2008, p. 106).

Os dados pessoais sensíveis, assim como qualquer dado pessoal, podem ser submetidos o tratamento. Neste sentido, o tratamento desses dados poderá ocorrer em apenas duas hipóteses expressamente previstas na LGPD: a) quando o titular do dado ou seu representante legal emitir o consentimento, sendo que este deverá ocorrer de forma específica e destacada, para finalidades que devem ser particularmente definidas; b) sem o consentimento do titular em algumas hipóteses em que isso for indispensável para finalidades específicas, como é o caso da proteção à saúde, quando o procedimento for realizado, exclusivamente por profissionais da saúde, serviços de saúde ou autoridade sanitária (art. 11, incisos I e II, “f”).

Segundo a LGPD, o consentimento é a manifestação livre, informada e inequívoca por meio da qual o titular concorda com o tratamento de seus dados

[Received/Recebido: Março 19, 2022; Accepted/Aceito: junho 15, 2022]

pessoais, sensíveis ou não, para uma finalidade determinada (art. 5º, inciso XII). Como se pode notar, o tratamento de dados pessoais sensíveis pode ser realizado mediante o consentimento do seu titular ou, em algumas hipóteses, sem o seu consentimento. O titular desses dados pode manifestar seu consentimento por si mesmo ou por meio do seu responsável legal (art. 11, I).

Vale reafirmar que esse consentimento deve ter forma específica e destacada e deve ser direcionado para finalidades específicas. Segundo a doutrina, *específico* é o consentimento manifestado em relação aos propósitos concretos e claramente determinados pelo controlador, antes mesmo do tratamento dos dados, ao passo que *destacado* diz respeito ao fato de ser importante que o titular tenha pleno acesso ao documento que informará todos os fatos relevantes sobre o tratamento de seus dados pessoais. Em outras palavras, o consentimento deve vir destacado, atendendo às disposições da lei, para que possa ter validade jurídica. “Além de se referir a dados determinados e haver declaração de vontade que esteja ligada a objetivo específico, a manifestação de vontade deverá vir em destaque no instrumento de declaração que autoriza o tratamento” (TEFFÉ, 2022, p. 137).

Vale ressaltar que, em relação ao consentimento do titular dos dados, aplicam-se também os requisitos de validade do negócio jurídico, exigindo-se a presença de agente capaz, objeto lícito, possível, determinado ou determinável e forma prescrita ou não defesa em lei (Código Civil, art. 104, incisos I, II e III). Desse modo, o consentimento do titular dos dados pessoais precisa obedecer aos critérios estabelecidos não apenas na LGPD, mas também no Código Civil brasileiro.

Por outro lado, pode haver situações em que ocorrerá o tratamento de dados pessoais sensíveis sem que haja a necessidade do consentimento do titular desses dados (art. 11, II). Isso ocorrerá, de modo excepcional, quando o tratamento dos dados for indispensável para a “tutela da saúde, exclusivamente, em procedimento realizado por profissionais da saúde, serviços de saúde ou autoridade sanitária” (art. 11, inciso II, alínea “f”).

É necessário destacar que todos os dados são importantes. Não existem dados pessoais desprovidos de valor. Por essa razão, todos os dados devem receber

[Received/Recebido: Março 19, 2022; Accepted/Aceito: junho 15, 2022]

tratamento adequado. Contudo, os dados pessoais sensíveis têm importância mais elevada.

> Naturalmente, contudo, o tratamento de dados sensíveis deve ser precedido de cautelas ainda maiores (com especial atenção aos princípios da lei e direitos dos titulares), uma vez que eventual incidente de segurança com os dados em referência pode trazer consequências mais gravosas aos direitos e às liberdades dos titulares (LIMA, 2021, p. 209).

A violação de um dado pessoal sensível, como é o caso da saúde, gera danos mais intensos ao seu titular, o que exige mais cuidado e proteção dos agentes de tratamento. Em outras palavras, o controlador e o operador devem atuar com mais zelo, quando o tratamento tiver por objeto dados pessoais sensíveis.

No que tange à realização de estudos em saúde pública, os órgãos de pesquisa estão autorizados por lei a terem acesso às bases de dados pessoais. Essa autorização se justifica pela necessidade de prevenir ou evitar danos de proporções coletivas.

Órgão de pesquisa, segundo a LGPD, com redação dada pela Lei n. 13.853, de 8 de julho de 2019, é o:

> órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico (art. 5º, inciso XVIII).

Os dados colhidos pelo órgão de pesquisa na realização de estudos em saúde pública não poderão ser tratados por outros órgãos ou utilizados para qualquer finalidade, mas exclusivamente dentro do órgão que os detiver e estritamente para a finalidade de realização de estudos e pesquisas, devendo, ainda, serem mantidos em ambiente controlado e seguro. Neste sentido, devem ser observadas as práticas de segurança previstas em regulamentos específicos sobre o tema, o que pode incluir a anonimização ou a pseudonimização dos dados, sempre com a observação dos devidos padrões éticos relacionados a estudos e pesquisas. A segurança da

[Received/Recebido: Março 19, 2022; Accepted/Aceito: junho 15, 2022]

informação deverá ser garantida pelo próprio órgão de pesquisa, não se permitindo, em nenhuma hipótese, a transferência dos dados a terceiros, seja pessoa física ou jurídica, seja esta de direito privado ou público.

Vale registrar, ainda, que, havendo divulgação dos resultados ou de qualquer excerto do estudo ou da pesquisa, não se poderá mencionar, em hipótese alguma, dados de natureza pessoal (art. 13, § 1º e 2º). É necessário, portanto, garantir um certo grau de sigilo e segurança em relação aos dados obtidos em razão de pesquisas realizadas no âmbito da saúde pública.

A atuação desses órgãos deve estar, adstritamente, vinculada aos diversos princípios estabelecidos pela LGPD, especialmente ao da finalidade. Esse princípio é definido como "a realização do tratamento para propósitos legítimos, específicos, explícitos e informados do titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades" (art. 6º, inciso II). Nota-se da definição do princípio de que os propósitos do tratamento dos dados devem ser legítimos, específicos, explícitos e informados. Em outras palavras, os agentes de tratamento (controlador e operador) estão vinculados a esses propósitos.

As condições estabelecidas para a realização de estudos em saúde pública foram sintetizadas por Konder (2020, p. 445):

> Reitera-se, de plano, a incidência do princípio da finalidade, ao determinar que o tratamento dos dados se restrinja à finalidade do estudo. Em proteção à segurança dos dados, determina-se que o tratamento somente ocorra dentro do órgão, impõe-se o respeito a práticas de segurança previstas em regulamentos específico e imputa-se ao órgão de pesquisa a responsabilidade pela segurança da informação, não permitida, em circunstância alguma, a transferência dos dados a terceiros. Impõe-se, ainda, que o tratamento deve respeitar os padrões éticos relacionados a estudos e pesquisas, como aqueles impostos pelo Comitê de Ética em Pesquisa (CEP) da instituição.

Os estudos em saúde pública podem ser realizados por diversos sujeitos, por órgãos públicos pertencentes à administração direta ou indireta de qualquer ente federativo, instituições privadas e, também, mediante parceria público-privada.

[Received/Recebido: Março 19, 2022; Accepted/Aceito: junho 15, 2022]

3 SEGURANÇA E SIGILO DE DADOS PESSOAIS SENSÍVEIS E PADRÕES DE BOAS PRÁTICAS E DE GOVERNANÇA

A LGPD impõe deveres aos agentes de tratamento (controlador e operador). Eles devem adotar medidas de segurança, técnicas e administrativas com aptidão para proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer outra forma de tratamento de dados feita inadequadamente ou de forma ilícita.

As medidas de segurança a serem adotadas pelos agentes de tratamento devem contemplar o princípio da segurança estabelecido na LGPG. Esse princípio consiste na "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" (art. 6º, inciso VII). As medidas técnicas, por outro lado, são as adotadas em Tecnologia da Informação, mediante a utilização de recursos informáticos dotados de funcionalidade e objetivando garantir a segurança da informação. Já as medidas administrativas são atividades desenvolvidas pelos agentes de tratamento, ou seja, aquelas medidas que consubstanciam o poder gerencial, envolvendo, portanto, a prática de atos jurídicos (JIMENE, 2021, p. 355-356).

Essas medidas a serem tomadas pelos controladores deverão ser observadas desde a fase de concepção do produto ou do serviço até o final da fase de sua execução (§ 2º), isto é, nas etapas relativas à concepção, ao desenvolvimento, à aplicação e à avaliação. Neste sentido, em relação à proteção de dados pessoais – portanto, também os dados pessoais sensíveis, como a saúde –, deve-se reconhecer que o Brasil adotou o conceito *privacy by design*, seguindo a trilha do Regulamento Geral de Proteção de Dados da Europa. Esse conceito foi criado em 1990 por Ann Cavoukian, então Comissária de Informação e Privacidade da Província de Ontário, no Canadá.

De acordo com o conceito *privacy by design*:

[Received/Recebido: Março 19, 2022; Accepted/Aceito: junho 15, 2022]

> [...] a privacidade deve ser protegida desde a concepção de um produto ou serviço, e que esta preferência deve ser mantida da mesma forma por todos os ciclos de desenvolvimento e inovação e ao longo das interações entre controladores e operadores e titulares de dados pessoais, como na obtenção de consentimento, na determinação de mecanismos de controle de dados e na delimitação das finalidades e do escopo do processamento (ARBIX, 2020, p. 56)

Para que esse objetivo seja alcançado, materializando a proteção dos dados pessoais sensíveis, compete à autoridade nacional estabelecer padrões técnicos mínimos, mas levando em consideração a natureza das informações tratadas, as características específicas do tratamento e o estado atual de desenvolvimento da tecnologia, especialmente, quando se tratar de dados pessoais sensíveis. Ademais, a autoridade nacional deverá observar os princípios inspiradores da LGPD, quais sejam: os princípios da boa-fé, finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização e prestação de contas (art. 46, § 1º).

Os sistemas informatizados utilizados para realizar o tratamento de dados pessoais, incluindo os dados pessoais sensíveis, como a saúde, devem ser estruturados com o objetivo de atender a diversas exigências, relativas aos requisitos de segurança, aos padrões de boas práticas e de governança, aos princípios gerais estabelecidos na LGPD e às demais normas que possam incidir sobre esses casos (art. 49).

Os requisitos de segurança são capazes de proteger os dados pessoais de acesso não autorizados, bem como de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer outra forma de tratamento inadequado ou ilícito. Os padrões de boas práticas e de governança devem levar em consideração a qualidade, a eficiência, a transparência e a ética de todo o processo de tratamento dos dados pessoais. Neste sentido, cabe à Autoridade Nacional de Proteção de Dados (ANPD) zelar pela manutenção de padrões elevados na proteção de dados pessoais, estabelecer diretrizes para a Política Nacional de Dados Pessoais e da Privacidade, bem como editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade (art. 55-J, incisos I, III e XIII). Já os princípios a serem observados são os

[Received/Recebido: Março 19, 2022; Accepted/Aceito: junho 15, 2022]

que estão estabelecidos no art. 6 da LGPD, acima referidos. Por último, as normas regulamentares são as que estão em vigência ou que venham a ser publicadas, com o propósito de ampliar e melhorar a disciplina jurídica sobre o tema.

Nesse contexto, o incidente de segurança é um acontecimento capaz de gerar consequências danosas aos dados pessoais, especialmente, os de natureza sensível:

> Em uma interpretação harmônica da LGPD, pode-se interpretar 'incidente de segurança' como um acontecimento indesejado ou inesperado, que seja hábil a comprometer a segurança dos dados pessoais, de modo a expô-los a acessos não autorizados e a situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito (JIMENE, 2021, p. 369-370).

Vale ressaltar que, diante da possibilidade de o incidente de segurança acarretar risco ou dano relevante aos titulares de dados pessoais, inclusive os de natureza sensível, o controlador deverá comunicar a situação à ANPD e ao titular dos dados. Todavia, não é qualquer incidente que obriga o controlador a praticar esse ato, mas um incidente de segurança grave, qualificado, com potencial para causar dano aos titulares dos dados pessoais.

> A identificação do incidente de segurança gerador do dever de informar é feita mediante a avaliação dos riscos eventualmente decorrentes do evento adverso. Devem-se considerar a gravidade das lesões potenciais aos direitos dos indivíduos e a probabilidade de ocorrerem. Logo, não é qualquer acontecimento adverso que impõe ao controlador a obrigação de comunicação à autoridade nacional e ao titular dos dados pessoais, mas, sim, o *incidente de segurança qualificado*, isto é, aqueles cuja probabilidade e gravidade dos riscos para os direitos e liberdades das pessoas naturais sejam aferíveis objetivamente a partir de considerações sobre a natureza, o âmbito, o contexto e as finalidades do tratamento, bem como sobre as características dos dados e de seus titulares (MODENESI, 2022, 452).

A comunicação deverá ser feita pelo controlador em prazo razoável e deverá conter, dentre outros, os seguintes dados e informações: a) a descrição da natureza dos dados pessoais afetados; b) as informações sobre os titulares envolvidos; c) a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial; d) os riscos relacionados ao incidente; e) os motivos da demora, no caso de a comunicação não ter sido imediata; e f) as

[Received/Recebido: Março 19, 2022; Accepted/Aceito: junho 15, 2022]

medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo (art. 40, § 1º, incisos I a VI).

Ao constatar a gravidade do incidente e objetivando proteger os direitos dos titulares dos dados, a ANPD poderá determinar que o controlador adote, imediatamente, algumas providências, tais como fazer ampla divulgação do fato em meios de comunicação e reverter ou mitigar os efeitos do incidente (art. 40, § 2º, incisos I e II).

A violação de dados pessoais, especialmente os de natureza sensível, pode acarretar responsabilidades aos agentes de tratamento. Essa responsabilidade pode ser de natureza administrativa, civil ou penal.

4 RESPONSABILIDADES ADMINISTRATIVA, CIVIL E PENAL DOS AGENTES DE TRATAMENTO DE DADOS PESSOIAS SENSÍVEIS

Os agentes de tratamento de dados desempenham papel fundamental e devem zelar pelos dados pessoais sensíveis. Todavia, quando violarem as normas previstas na LGPD, podem ficar sujeitos às sanções administrativas, civis e penais. As duas primeiras espécies de sanção estão previstas na LGPD, ao passo que a sanções penais pertencem a outros corpos legislativos.

As sanções administrativas são a advertência, a multa simples, a multa diária, a publicização da infração, o bloqueio dos dados pessoais e a eliminação dos dados pessoais (art. 52).

A advertência pode ser verbal ou por escrito. Trata-se de uma sanção de natureza leve, que transporta um caráter pedagógico. Ela não pode ser indefinida no tempo, mas conter um prazo determinado para que o infrator realize as medidas corretivas (art. 52, inciso I).

A multa simples pode chegar até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado. O percentual deve levar em consideração o último exercício financeiro, excluídos os tributos. A multa deve ser limitada, por infração, ao valor de R$ 50.000.000,00 (cinquenta milhões de reais). No

[Received/Recebido: Março 19, 2022; Accepted/Aceito: junho 15, 2022]

cálculo da multa, a autoridade nacional poderá considerar o faturamento total da empresa ou grupo de empresas em três hipóteses: a) quando não dispuser do valor do faturamento no ramo da atividade empresarial em que ocorre a infração; b) quando o valor for apresentado de forma incompleta; c) quando o valor não for demonstrado de forma inequívoca e idônea (art. 52, inciso II, § 4º).

A multa diária, também conhecida como *astreinte*, deve ter como limite total o valor de R$ 50.000,00 (cinquenta mil reais) (art. 52, inciso III).

A publicização da infração cometida pelos agentes de tratamento de dados pode se dar de várias formas, atendendo ao princípio constitucional da publicidade dos atos da administração pública (art. 37). Contudo, somente será admitida essa publicização, após a realização de processo administrativo, com todas as garantias que este exige. Em outras palavras, para que seja aplicada essa sanção, é necessário que a infração tenha sido apurada, mediante procedimento regular, e que sua ocorrência resulte confirmada.

O bloqueio dos dados pessoais é de difícil ocorrência no campo prático, visto que os dados estão disponibilizados no espaço virtual. Parece não ser possível evitar que os dados sejam acessados.

Em relação à sanção que objetiva eliminar os dados pessoais, as dificuldades são semelhantes. Eliminar significa apagar, assegurando-se que os dados não serão recuperados. Se os dados pessoais já foram replicados, todavia, a sua eliminação poderá ter efeitos bastante limitados.

Qualquer uma das sanções acima referidas somente poderá ser aplicada após a realização do adequado procedimento administrativo, no qual se tenham asseguradas as garantias processuais. A sanção deve ser aplicada de acordo com as peculiaridades do caso concreto, levando-se em consideração os seguintes parâmetros e critérios: a) a gravidade e a natureza das infrações e dos direitos pessoais violados; b) a boa-fé do infrator; c) a vantagem auferida ou pretendida pelo infrator; d) a condução econômica do infrator; e) a reincidência; f) o grau do dano; g) a cooperação do infrator; h) a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano; i) a adoção de política de boas

[Received/Recebido: Março 19, 2022; Accepted/Aceito: junho 15, 2022]

práticas corretivas; j) a proporcionalidade entre a gravidade da falta e a intensidade da sanção (art. 53, § 1º).

As sanções administrativas podem ser aplicadas pela autoridade administrativa competente ou pelo Poder Judiciário. No âmbito administrativo, a Autoridade Nacional de Proteção de Dados (ANPD) tem competência para fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação, o que deverá ser feito mediante um processo administrativo que assegure todas as garantias constitucionais, entre elas, o contraditório, a ampla defesa e o direito de recurso" (art. 55-J, inciso IV). É importante ressaltar que a competência atribuída a ANPD para aplicar sanções previstas na LGPD, no que tange à proteção de dados pessoais, incluindo os de natureza sensível, tem preferência em relação a outras entidades ou órgãos da administração pública (art. 55-K), tais como o CADE – Conselho Administrativo de Defesa Econômica e o PROCON – Órgão de Defesa e Proteção do Consumidor.

A importância do papel desempenhado pela ANPD, especialmente, o de fiscalizar e sancionar, tem sido destacada pela doutrina:

> De grande importância a atividade fiscalizatória e, de conseguinte, sancionatória. Está prevista no inciso IV do art. 55-J da LGPD, incidindo na hipótese de descumprimento dos dispositivos desta. Manifesta-se mediante procedimento administrativo, no qual assegurados o contraditório, a ampla defesa e o direito de interpor recursos (NOBRE JÚNIOR, 2020, p. 577).

No exercício de atividade de tratamento dos dados pessoais sensíveis, tanto o controlador como o operador podem causar danos ao titular desses dados. Em ocorrendo o dano patrimonial ou moral, em dimensões individual ou coletiva, impõe-se o dever de repará-los, visto que cada qual responde por seus atos. Todavia, o operador responde solidariamente com o controlador pelos danos causados em virtude do tratamento dos dados, em duas hipóteses: a) quando descumprir a legislação de proteção de dados; b) quando não tiver seguido as orientações lícitas dadas pelo controlador. No mesmo sentido, o controlador irá responder solidariamente com o operador pelos danos causados ao titular dos dados, quando estiver

[Received/Recebido: Março 19, 2022; Accepted/Aceito: junho 15, 2022]

diretamente envolvido no tratamento dos dados (art. 42, § 1º, inciso I e II). Vale ressaltar, todavia, que, nos casos acima referidos, não incidirá a responsabilidade civil dos agentes de tratamento, nas hipóteses em que a LGPD prever a exclusão de responsabilidade (art. 43).

A LGPD não foi explícita no que tange à natureza da responsabilidade civil, abstendo-se de indicar se é objetiva ou subjetiva. Acredita-se, inclusive, que ela o fez deliberadamente, deixando para o intérprete e aplicador do direito identificar em outros campos do ordenamento jurídico brasileiro qual tipo de responsabilidade civil deverá ser adotada. Assim, é necessário localizar a solução em diversos corpos normativos, tais como o Código de Defesa do Consumidor (art. 14) Código Civil (art. 186) e a Constituição Federal (art. 37, par. 6º).

É preciso distinguir a responsabilidade civil dos estabelecimentos de saúde (hospitais, laboratórios de análises clínicas) da responsabilidade civil do profissional liberal. Na primeira hipótese, a responsabilidade será objetiva, aplicando-se o art. 14 do CDC. Portanto, o dever de indenizar decorre do risco da atividade, não sendo exigível a comprovação da culpa (negligência, imprudência, imperícia). Na segunda hipótese, em que o dano é causado por profissional liberal, a responsabilidade será subjetiva, incidindo a norma específica do art. 14, par. 4º, do CDC. Nesta hipótese, o dever de reparar o dano somente irá incidir se ficar demonstrado que o profissional liberal procedeu com culpa.

Neste sentido, segundo a lição da doutrina:

> Por exemplo, um vazamento de prontuários médicos de um hospital ou dos resultados de exames realizados por um laboratório, resta evidente que a responsabilidade destes estabelecimentos será objetiva. Entretanto, o mesmo vazamento de dados de prontuários armazenados por um médico em seu consultório resultará em apuração da culpa, por ser este um profissional liberal (THOMASEVICIUS FILHO, 2021, p. 214).

Contudo, se não houver relação de consumo, as normas do CDC não serão aplicadas. Pode ocorrer, então, que, na aferição de existência de responsabilidade civil do causador do dano, tenha que ser aplicada a norma do Código Civil que trata

[Received/Recebido: Março 19, 2022; Accepted/Aceito: junho 15, 2022]

da responsabilidade civil subjetiva, isto é, deverá haver a comprovação da culpa (art. 186).

Por outro lado, quando o tratamento dos dados pessoais sensíveis for realizado no âmbito do poder público (no SUS, por exemplo), a responsabilidade será objetiva (FACHIN, 2001, p. 109-115). Nessa hipótese, a responsabilidade será objetiva em face da relação titular dos dados e poder público, cabendo a este o direito de regresso em relação ao causador do dano (prestador de serviço público), exigindo-se, nesta hipótese, a prova de dolo ou culpa, por força da norma inserida no art. 37, par. 6º, da Constituição Federal.

A ação de indenização deve ser ajuizada pelo titular do direito lesado, que é o titular dos dados pessoais sensíveis. No polo passivo, deverão figurar o operador e o controlador. Entre esses, a responsabilidade é solidária, por expressa previsão da LGPD (art. 42, § 1º, incisos I e II). Sendo a responsabilidade solidária, qualquer um dos causadores do dano responderá pela integralidade do valor a ser indenizado. Em outras palavras, o autor da ação de indenização poderá exigir de qualquer dos agentes de tratamento (operador e controlador) a totalidade do débito apurado.

Observa-se que o dano indenizável não é apenas o de efeito individual, mas, também, o coletivo. Neste contexto, a ação de reparação de danos pode ser exercida coletivamente em juízo, observando-se a Constituição Federal, legislação específica sobre o processo coletivo e a própria LGPD (art. 42, § 3º).

Deve-se acrescentar, ainda, que o dano a ser indenizado pode ser material ou moral, ou ambos, conjuntamente. Em situações específicas, tendo em vista que a saúde é um dado pessoal sensível, pode ser que, além dos danos material e moral, ocorra também um dano à imagem, compreendida como imagem-reputação, capaz de atingir a honra da pessoa titular dos dados violados (Constituição Federal, art. 5º, inciso V).

Ademais, vale registrar que, no âmbito do processo civil, o juiz poderá inverter o ônus da prova a favor do titular dos dados supostamente violados, quando se apresentar uma das seguintes circunstâncias: a) a alegação de dano e autoria for verossímil; b) houver hipossuficiência para fins de produção de prova; c) a produção de provas por parte do titular dos dados for excessivamente onerosa (art. 42, § 2º).

[Received/Recebido: Março 19, 2022; Accepted/Aceito: junho 15, 2022]

Um aspecto importante a ser destacado é que o titular dos dados pessoais sensíveis deve ser considerado, sempre, como hipossuficiente, visto que não tem qualquer poder em face dos agentes de tratamento (operador e controlador).

Por outro lado, ressalta-se que o controlador e o operador poderão provar a existência de exclusão de ilicitude, caso em que não serão responsabilizados patrimonialmente. Em outras palavras, nenhum deles responderá pelos danos materiais ou morais ao titular dos dados pessoais sensíveis, se provarem a existência de uma das seguintes excludentes: a) não realizaram o tratamento de dados pessoais que lhes é atribuído; b) embora tenham realizado o tratamento de dados a eles atribuído, não ocorreu violação à legislação de proteção de dados pessoais; c) o dano decorreu por culpa exclusiva do titular dos dados ou de terceiros (art. 43).

Vale registrar que, além da responsabilidade administrativa e civil, os agentes de tratamento causadores de ato ilícito poderão sofrer também sanções penais. Isto significa reconhecer que os agentes de tratamento de dados pessoais gerais ou sensíveis podem ser penalmente responsabilizados por condutas que se amoldem a tipos penais. Tornou-se comum, no âmbito do ciberespaço, a prática de delitos. Em outras palavras, esse espaço virtual "vem se tornando cada vez mais sítio de conflitos, que por muitas vezes terminam em difusão de um ato ilícito civil ou até mesmo delitos tipificados no Código Penal" (LÓSSIO; SANTOS, 2020, P. 402).

Pode-se afirmar que se está diante de uma nova realidade do Direito Criminal, pois se trata de um Direito Criminal Digital Difuso, visto que essa criminalidade digital é pluriofensiva e transnacional (FULLER, 2020, p. 379-399). Vale ressaltar que, embora a LGPD não tenha tratado de matéria penal, os atos praticados no espaço virtual podem ser subsumidos a tipos penais descritos em outros corpos normativos, especialmente, o Código Penal brasileiro.

Diante dessa nova realidade, o legislador brasileiro introduziu algumas inovações no âmbito da cibe criminalidade. Por exemplo, a Lei 9.459, de 13 de maio de 1997, acrescentou o § 2º ao artigo 20 da Lei 7.716/1989 (delito de praticar, induzir ou incitar a discriminação ou preconceito de raça, cor, etnia, religião ou procedência nacional), que traz uma nova qualificadora quando as condutas descritas no *caput* forem praticadas por "intermédio dos meios de comunicação social ou publicação de

[Received/Recebido: Março 19, 2022; Accepted/Aceito: junho 15, 2022]

qualquer natureza". Ainda com relação a tal delito, a Lei 12.735, de 30 de novembro de 2012, deu nova redação ao § 3º, inciso II, do citado art. 20, conferindo ao juiz a possibilidade de determinar, na hipótese de crime cometido por intermédio dos meios de comunicação social ou outra publicação, a "cessação das respectivas transmissões radiofônicas, televisivas, eletrônicas ou da publicação por qualquer meio".

Na mesma data, foi publicada a Lei 12.737/2012, denominada "Lei Carolina Dieckman", que alterou alguns dispositivos do Código Penal. A modificação de maior destaque foi a tipificação do artigo 154-A do Código Penal (invasão de dispositivo informático). Este artigo, recentemente alterado pela Lei 14.155/2021, incrimina a conduta de "invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita". As penas atualmente previstas são a reclusão, de um a quatro anos, e a multa.

Além desses dispositivos, alguns outros crimes podem ser destacados. Por exemplo, no delito de inserção de dados falsos em sistema de informações (art. 313-A, incluído pela Lei 9.983/2000), tipifica-se a conduta de "inserir ou facilitar, o funcionário autorizado, a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos sistemas informatizados ou bancos de dados da Administração Pública com o fim de obter vantagem indevida para si ou para outrem ou para causar dano". As penas cominadas são a reclusão, de dois a doze anos, e a multa.

Nesse mesmo contexto, o Código Penal prevê ser crime de violação de sigilo funcional a realização das seguintes condutas: a) revelar fato de que tem ciência em razão do cargo e que deva permanecer em segredo, ou facilitar-lhe a revelação; b) permitir ou facilitar, mediante atribuição, fornecimento e empréstimo de senha ou qualquer outra forma, o acesso de pessoas não autorizadas a sistemas de informações ou banco de dados da Administração Pública; c) utilizar-se, indevidamente, do acesso restrito. As penas previstas são de detenção, de seis meses a dois anos, ou de multa (art. 325, CP).

[Received/Recebido: Março 19, 2022; Accepted/Aceito: junho 15, 2022]

Muitas das condutas tipificadas nas leis acima referidas, uma vez realizadas pelos agentes de proteção de dados pessoais, podem violar dados pessoais sensíveis, inclusive, o relativo à saúde.

Conclui-se, então, que o controlador e o operador, agentes de tratamento de dados pessoais sensíveis, podem se submeter à tríplice responsabilidade: administrativa, civil e penal.

4 CONSIDERAÇÕES FINAIS

A LGPD estabeleceu ampla proteção dos dados pessoais e faz distinção entre dados pessoais gerais e dados pessoais sensíveis. Os primeiros são qualquer dado relativo à pessoa humana, já os dados pessoais sensíveis referem-se aos aspectos específicos da existência humana, tais como origem racial ou ética, convicção religiosa, opinião política, filiação à sindicato ou à organização de caráter religioso, filosófico ou político, à saúde ou à vida sexual, bem como aos dados genéticos ou biométricos, quando vinculados a uma pessoa natural. Esses dados, por seu caráter essencial, devem receber proteção jurídica mais qualificada e eficaz.

A mencionada lei tratou de uma pluralidade de temas, especialmente, da segurança e do sigilo dos dados pessoais sensíveis e dos padrões de boas práticas e de governança. Essas normas precisam ser observadas pelos agentes de tratamento (operador e controlador), sob pena de responsabilização.

O consentimento do titular dos dados pessoais tem valor extraordinariamente importante no processo de tratamento desses dados. Salvo exceções estabelecidas pela própria LGPD, não pode haver tratamento de dados pessoais gerais sem o consentimento do seu titular. No que tange aos dados pessoais sensíveis, o legislador foi ainda mais restritivo.

O controlador e operador, habilitados a realizarem tratamentos de dados pessoais, especialmente os de natureza sensível, assumem enormes responsabilidades na proteção desses dados, podendo ser compelidos a responderem pelos danos decorrentes de suas atividades.

[Received/Recebido: Março 19, 2022; Accepted/Aceito: junho 15, 2022]

Neste sentido, os agentes de tratamento estão submetidos à tríplice responsabilidade: administrativa, civil e penal, ainda que a responsabilidade penal não decorra da LGPD, mas de outros corpos normativos. Essas três reponsabilidades, inclusive, podem incidir de modo cumulativo.

Desse modo, a pesquisa reconhece que a LGPD protege adequadamente os dados pessoais sensíveis. Contudo, adverte para a necessidade de os agentes de tratamento, bem como empresas, instituições e governos, estarem comprometidos com a efetivação das suas normas.

REFERÊNCIAS

ARBIX, Daniel. A Importância da Privacidade por *Design* e por Defaut (*Privacy by Design and by Defaut*). In: DONEDA, Danilo; MENDES, Laura Schertel; CUEVA, Ricardo Villas Bôas. **Lei Geral de Proteção de Dados** (Lei 13. 709/2018): a caminho da efetividade: contribuições para a implementação da LGPD. São Paulo: Thomson Reuters Brasil, 2020, p. 55-63.

COLOMBO, Cristiano. Disposições Preliminares. In: MARTINS, Guilherme Magalhães. LONGHI, João Victor Rozatti; FALEIROS JÚNIOR, José Luiz de Moura (Coordenadores). **Comentários à Lei Geral de Proteção de Dados Pessoais**. Indaiatuba, SP: Foco, 2022, p. 1-18.

FACHIN, Zulmar. **Responsabilidade Patrimonial do Estado por Ato Jurisdicional**. Rio de janeiro: Renovar, 2001.

FULLER, Greice Patrícia. Crimes na Sociedade da Informação: uma nova realidade fenomênico-jurídica. In: LISBOA, Roberto Senise (coordenador). **O Direito na Sociedade da Informação IV**: movimentos sociais, tecnologia e a atuação do Estado. São Paulo: Almedina, 2020, p. 379-399.

JIMENE, Camilla do Valle. Da Segurança e do Sigilo de Dados. In: MALDONADO, Viviane Nóbrega; OPICE BLUM, Renato. **LGPD**: Lei Geral de proteção de Dados Comentada. 3. ed. São Paulo: Thomson Reuters Brasil, 2021, p. 355-386.

KONDER, Carlos Nelson. O Tratamento de Dados Sensíveis à Luz da Lei 13.709/2018. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. **Lei Geral de Proteção de Dados Pessoais e suas Repercussões no Direito brasileiro**. 2. ed. São Paulo: Thomson Reuters Brasil, 2020, p. 441-459.

[Received/Recebido: Março 19, 2022; Accepted/Aceito: junho 15, 2022]

LIMA, Caio César Carvalho. Do Tratamento de Dados Pessoais Sensíveis. In: MALDONADO, Viviane Nóbrega; OPICE BLUM, Renato. **LGPD**: Lei Geral de proteção de Dados Comentada. 3. ed. São Paulo: Thomson Reuters Brasil, 2021, p. 209-220.

LÓSSIO, Cláudio Joel Brito; SANTOS, Cariolano Aurélio Almeida Camargo. Cultura da Paz e Soberania no Ciberespaço em Face do Cibercrime. In: In: LISBOA, Roberto Senise (coordenador). **O Direito na Sociedade da Informação IV**: movimentos sociais, tecnologia e a atuação do Estado. São Paulo: Almedina, 2020, p. 401-418.

MODENESI, Pedro. Da Segurança e do Sigilo de Dados. In: MARTINS, Guilherme Magalhães; LONGHI, João Victor Rozatti; FALEIROS JÚNIOR, José Luiz de Moura (Coordenadores). **Comentários à Lei Geral de Proteção de Dados Pessoais**. Indaiatuba, SP: Foco, 2022, p. 431-460

NOBRE JÚNIOR, Edilson Pereira. A Autoridade Nacional de Proteção de Dados Pessoais e o Dever Estatal de sua Tutela: anotações em torno da independência do órgão regulador. In: POZZO, Augusto Neves dal; MARTINS, Ricardo Marcondes. **LGPD e Administração Pública**: uma análise ampla dos impactos. São Paulo: Thomspn Reuters Brasil, 2020, p. 560-584.

PALMEIRA, Mariana de Moraes. Do Tratamento de Dados Pessoais Sensíveis. In: MARTINS, Guilherme Magalhães; LONGHI, João Victor Rozatti; FALEIROS JÚNIOR, José Luiz de Moura (Coordenadores). **Comentários à Lei Geral de Proteção de Dados Pessoais**. Indaiatuba, SP: Foco, 2022, p. 149-166.

RODOTÁ, Stefano. **A Vida na Sociedade da Vigilância**: a privacidade hoje. Trad.: Danilo Doneda a Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

TEFFÉ, Chiara Spadaccini. Do Tratamento de Dados Pessoais Sensíveis. In: MARTINS, Guilherme Magalhães; LONGHI, João Victor Rozatti; FALEIROS JÚNIOR, José Luiz de Moura (Coordenadores). **Comentários à Lei Geral de Proteção de Dados Pessoais**. Indaiatuba, SP: Foco, 2022, p. 126-148

THOMASEVICIUS FILHO, Eduardo. Responsabilidade Civil na LGPD na Área da Saúde. In: DALLARI, Analluza Bolívar; MONACO, Gustavo Ferraz de Campos. **LGPD na Saúde** (Coordenação). São Paulo: Thomson Reuters Brasil, 2021, p. 211-222.

VIOLA, Mario. TEFFÉ, Chiara Spadaccini de. Tratamento de Dados Pessoais na LGPD: estudo sobre as bases legais dos artigos 7º e 11. In: MENDES, Laura Schertel *et al*. **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense, 2021, p. 117-148.

[Received/Recebido: Março 19, 2022; Accepted/Aceito: junho 15, 2022]