O REGIME DE RESPONSABILIZAÇÃO CIVIL NA LEI GERAL DE PROTEÇÃO DE DADOS

Gilberto Bomfim[1]

Resumo: Seguindo uma tendência mundial iniciada com o advento do Regulamento Geral sobre a Proteção de Dados da União Européia (*General Data Protection Regulation*), o Brasil aprovou a Lei nº 13.709/2018, denominada Lei Geral de Proteção de Dados Pessoais (LGPD). A LGPD define os requisitos para o tratamento e compartilhamento de dados pessoais, elenca os direitos de seus titulares e as medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais, bem como estabelece o regime de responsabilidade civil por violação da lei e ressarcimento de danos. Nesse contexto, o artigo tem por objetivo avaliar o regime de tratamento e compartilhamento de dados pelo Poder Público na LGPD. Utilizando-se do método hipotético-dedutivo, o problema a ser enfrentado é identificar o regime de responsabilização civil trazido pela lei para os casos de violação aos deveres por ela impostos, com ênfase para as disposições aplicáveis à Administração Pública. Ao final, conclui-se que o legislador optou pela regra geral da responsabilidade civil subjetiva (arts.42 e seguintes da LGPD). No que toca à responsabilização civil da Administração Pública, por outro lado, ausência opção expressa do legislador, a doutrina e a jurisprudência ainda estão divididas entre a regra da responsabilidade subjetiva (prevista art.42 da LGPD) ou da responsabilidade objetiva, independentemente de culpa (cf. art. 37, § 6º, da CF).

Palavras-Chave: Lei Geral de Proteção de Dados. Administração Pública. Danos. Responsabilidade Subjetiva. Ressarcimento.

[1] Mestre em Direito Econômico e Desenvolvimento pela Pontifícia Universidade Católica do Paraná - PUCPR.

Sumário: Introdução; 1. As hipóteses legais de tratamento de e compartilhamento de dados pessoais na LGPD; 2. A segurança e o sigilo dos dados na LGPD; 3. O regime de responsabilização civil na LGPD. Considerações finais. Referências.

INTRODUÇÃO

tema relativo à proteção de dados pessoais possui *status* constitucional**,** sendo, até muito recentemente, considerado implicitamente reconhecido pelo ordenamento jurídico em decorrência do direito fundamental à intimidade, à vida privada, à honra e à imagem das pessoas (art.5o, inciso X, CF). Entretanto, com o advento da Emenda Constitucional n. 115/2022, tal previsão passa a ser expressa com a inclusão do inciso LXXIX, segundo o qual "é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais" (BRASIL, 1988).

Paralelamente, no âmbito infraconstitucional, até agosto de 2018*, o Brasil contava com variadas normas relativas a questões relacionadas à privacidade e à proteção de dados pessoais*, como o Código de Defesa do Consumidor (Lei 8.078/1990), a Lei de Acesso à Informação (Lei 12.527/2011), a Lei do Cadastro Positivo (Lei 12.414/2011) e o Marco Civil da Internet (Lei 12.965/2014). Contudo, como aponta a doutrina[2], esse arcabouço regulatório mostrava-se pouco preciso e não oferecia as garantias adequadas para a sociedade, de modo que se faziam necessários métodos hermenêuticos como a analogia e a análise

[2] Para maiores detalhes vide: XAVIER, Luciana Pedroso; XAVIER, Marília Pedroso; SPALER, Mayara Guibor. Primeiras impressões sobre o tratamento de dados pessoais nas hipóteses de interesse público e execução de contratos. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coord.). *Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro*. 2a. Ed. São Paulo: Thompson Reuters Brasil, 2020. p.479-497.

sistemática para viabilizar a sua aplicação.

Com efeito, seguindo uma tendência mundial iniciada após o advento do Regulamento Geral sobre a Proteção de Dados da União Européia (*General Data Protection Regulation*) - legislação que serviu de parâmetro para a elaboração do marco regulatório nacional, *o Brasil aprovou a Lei nº 13.709/2018*, denominada Lei Geral de Proteção de Dados Pessoais (LGPD), que dispõe sobre o tratamento de dados pessoais, tanto nos meios físicos e digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com a finalidade de proteger os direitos fundamentais da liberdade e da privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Todos os *direitos* dos titulares dos dados pessoais elencados pela lei vem associados de uma série de *deveres* daqueles que exercem a atividade de tratamento de dados e que, por consequência, estão submetidos à *responsabilização administrativa e civil* quando descumprem tal legislação. Ademais, a LGPD distingue o tratamento de dados pessoais pelo poder público (arts. 23-30) com sua respectiva seção de responsabilidade (arts. 31 e 32) dos agentes de tratamento de dados pessoais, com sua respectiva seção de responsabilidade (arts. 42-45). O legislador optou, portanto, por uma separação dos sujeitos de direito e de sua respectiva responsabilização, em seu âmbito público e privado.

Nesse contexto, o artigo tem por *objetivo* avaliar o regime de tratamento e compartilhamento de dados pelo Poder Público na Lei Geral de Proteção de Dados. Utilizando-se do *método hipotético-dedutivo*, o *problema* enfrentado é identificar o regime de responsabilização dos agentes de tratamento de dados pessoais por violação aos deveres a ele impostos pela Lei, com ênfase para as disposições aplicáveis à Administração Pública.

Para tanto, o artigo está estruturado da seguinte forma: No capítulo 1 serão avaliadas as hipóteses legais autorizadoras de tratamento e compartilhamento de dados pessoais, bem como

sua aplicação ao Poder Público. No capítulo 2 serão tratadas as normas relativas à segurança e ao sigilo dos dados pessoais na LGPD. O capítulo 3 tratará do regime de responsabilização dos agentes de tratamento em caso de violação dos deveres estipulados na LGPD.

As considerações finais apontam as respostas encontradas para o problema da pesquisa, traçando uma linha lógica para demonstrar o cumprimento do objetivo geral do trabalho.

1. AS HIPÓTESES LEGAIS DE TRATAMENTO E COMPARTILHAMENTO DE DADOS PESSOAIS NA LGPD

Considerando a necessidade de se dar proteção jurídica aos direitos à privacidade e à proteção de dados pessoais, foram elaboradas no Brasil e ao redor do mundo diversas legislações com o objetivo de regulamentar o acesso, tratamento e o compartilhamento de dados pessoais (BOMFIM; CASTRO, 2020, p.72)

No Brasil, a Lei Geral de Proteção de Dados (Lei n. 13.709/2018) versa sobre o *tratamento de dados pessoais* de pessoas naturais, tanto em meio físico quanto digital, com a finalidade de garantir seus direitos fundamentais a liberdade, privacidade e o livre desenvolvimento da personalidade, assim considerado em seu art.5o, X, como sendo

> toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração (art.5o, X).

A *definição de tratamento de dados trazida pela lei é extremamente abrangente***,** partindo da coleta e findando com a eliminação dos dados pessoais, englobando todas as opções de manuseio e compartilhamento, não importando o meio utilizado (PIRONTI; ZILIOTTO, 2021, p.412). Logo, percebe-se que *a*

Lei Geral de Proteção de Dados pretendeu regular todas as formas de tratamento de dados pessoais, como quaisquer informações relacionadas à pessoa natural identificada ou identificável (art.5o, I), incluindo até mesmo aqueles considerados públicos ou tornados públicos pelos titulares.

Ana Frazão (2020, p.101) ensina que a LGPD acolheu uma concepção que considera que "a proteção de dados corresponde a verdadeiro direito fundamental autônomo, expressão da liberdade e da dignidade humana, que está intrinsecamente relacionada à impossibilidade de transformar os indivíduos em objeto de vigilância".

Nesse contexto, ao dispor sobre o tratamento de dados, a LGPD prevê, em seu art.7º, as *hipóteses legais que autorizam o tratamento de dados pessoais*.

A primeira hipótese que autoriza o tratamento dos dados é *o consentimento do titular* das informações pessoais, disciplinado no artigo 5o, inciso XII, da LGPD, o qual deve consistir em manifestação livre, informada e inequívoca pelo titular dos dados, no sentido de concordar com o tratamento de seus dados pessoais para uma finalidade determinada. Deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular (art.8º)[3]. A lei não exige, portanto, o consentimento escrito, mas, caso assim ele seja colhido, deverá constar em cláusula destacada das demais cláusulas contratuais (TEPEDINO, TEFFÉ, 2021, p.297)[4].

[3] Elenca o Manual da Legislação Europeia sobre Proteção de Dados três elementos de um consentimento válido que assegura que as pessoas objeto de tratamento de dados genuinamente autorizam a sua utilização. 1) a pessoa não pode estar sob qualquer pressão quando presta o seu consentimento, assemelhando-se ao disposto no art. 8°, §3° da Lei 13.709, porém este mais completo; 2) a pessoa em causa deve ter sido devidamente informada sobre o objeto e as consequências do consentimento; e 3) o âmbito do consentimento deve ser razoavelmente concreto; sendo tais requisitos aplicáveis de forma cumulativa, condicionando o consentimento válido somente se observado todos os três requisitos acima citados (UNIÃO EUROPEIA, 2014, p. 59).

[4] Embora não precise necessariamente estar consubstanciado em declaração escrita, o consentimento não poderá ser extraído da omissão do titular, mas tão somente de atos que revelem claramente sua real vontade (TEPEDINO, TEFFÉ, 2021, p.297).

As demais hipóteses que autorizam o tratamento de dados (incisos II a X) independem do consentimento do titular referem-se i) ao cumprimento de obrigação legal ou regulatória pelo controlador, como no caso de provedores de aplicações de internet que precisam manter seus registros de acesso pelo prazo de 6 meses (art.15, da Lei 12.925/2014); ii) a realização de estudos por órgão de pesquisa, iii) a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados; iv) ao exercício regular de direitos em processo judicial, administrativo ou arbitral, v) a proteção da vida ou da incolumidade física do titular ou de terceiros; vi) a tutela da saúde; vii) ao atendimento aos interesses legítimos do controlador ou de terceiro, viii) a proteção do crédito, e ix) ao tratamento e uso compartilhado de dados pela administração pública, necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres[5].

Sthéfano Divino e Taisa Lima (2020, p.10) esclarecem que, caso configurada qualquer uma das hipóteses presente nos incisos II a X, estará autorizado o tratamento de dados, independentemente de ter ou não o consentimento do titular.

Ao afirmar que os dados pessoais somente podem ser tratados em determinadas hipóteses, a LGPD estabeleceu um *rol taxativo*, demonstrando a preocupação e seriedade com o tratamento do assunto. Contudo, mister ressaltar a grande amplitude decorrente das *previsões generalizantes* que viabilizam o enquadramento de inúmeras situações nas citadas hipóteses da legislação brasileira (XAVIER; XAVIER; SPALER, 2020, p.490).

Dentre as hipóteses legais de tratamento generalizantes e que dispensam o consentimento do titular, a LGPD conferiu *amplos e discricionários poderes à Administração Pública para*

[5] Observe-se, contudo, que mesmo nos casos de dispensa da exigência do consentimento do titular, os agentes de tratamento continuarão obrigados com as demais disposições previstas na lei.

realizar o tratamento de dados pessoais considerados necessários à execução de políticas públicas previstas em lei e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres (art.7º, II).

Com efeito, a**s** hipóteses em que o consentimento será necessário para o tratamento dos dados pela Administração Pública são excepcionais**,** isto é, quando não estiver albergado na hipótese legal do art.7o, incisos II.

Isso porque *a Administração Pública exerce ampla gama de atividades administrativas e implementa políticas públicas em cumprimento do interesse público*. É incontestável, portanto, que a criação e execução de muitas políticas públicas poderiam ser comprometidas pela falta de informações relevantes pelo Poder Público. Com efeito, *não se pode olvidar que um dos maiores interessados na coleta de dados pessoais é a própria Administração Pública*, que exige dos titulares a exposição constante e crescente de suas informações pessoais para fins de execução daquelas políticas públicas (PIRONTI, ZILIOTTO, 2021, p. 419).

Danilo Doneda (2020, p.34), ao abordar os motivos utilizados pelo Estado para a utilização de dados pessoais, ensina que

> Em primeiro lugar, foi o Estado que por primeiro se encontrou na posição de utilizar largamente informações pessoais. Os motivos são razoavelmente claros: um pressuposto para uma administração pública eficiente é o conhecimento tão acurado quanto possível da população (não por acaso, à formação do *welfare state* seguiu-se um período de voraz demanda por informação pessoal por parte do Estado), o que implica, por exemplo, a realização de censos e pesquisas e o estabelecimento de regras para tornar compulsória a comunicação de determinadas informações pessoais à administração pública. Em relação ao controle, basta acenar às várias formas de controle social que podem ser desempenhadas pelo Estado e que seriam potencializadas com a maior disponibilidade de informações sobre os cidadãos, aumentando seu poder sobre os indivíduos – não é por outro motivo que um forte controle da informação

> é característica comum aos regimes totalitários (DONEDA, 2020, p.34).

Outrossim, a LGPD estabelece que o tratamento de dados pelo Poder Público "*deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público*" (art.23, LGPD). Para isso, como observado por Xavier, Xavier e Spaler (2020, p.491), a LGPD estabeleceu algumas condições, tais como: i) observância das hipóteses legais para tratamento; ii) informação clara em veículos oficiais de fácil acesso, sobre tal previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades; e iii) indicação de um encarregado quando da realização de operações de tratamento de dados pessoais.

Outro ponto importante é que os dados pessoais envolvidos nos tratamentos efetuados pela Administração Pública deverão ser mantidos em *formato interoperável e estruturado para seu compartilhamento* (art.25, LGPD), ou seja, devem ser armazenados de forma que facilite sua transferência para outras entidades vinculadas e que simplifique os processos internos (BOSTELMANN; MAFRA, 2021, p.144).

Essa facilitação se dá para que se alcance de maneira mais eficiente a execução de políticas públicas, a prestação de serviços públicos, bem como ocorra uma descentralização da atividade pública de maneira mais coerente e segura. Por fim, a simplificação ajudará também na disseminação e acesso das informações ao público, assim garantindo os direitos de todos os titulares envolvidos (BOSTELMANN; MAFRA, 2021, p.145).

O compartilhamento de dados pessoais pelo Poder Público é, em regra, permitido apenas entre os órgãos públicos e só poderá ser concedido quando os dados tratados forem necessários para elaboração de políticas públicas ou quando houver determinação legal para tanto.

Já a transferência dos dados pessoais obtidos pelo Poder

Público às entidades privadas é vetada, com exceção das situações em que os dados são acessíveis publicamente ou em que a execução de um serviço ou medida o exigir. Nesse sentido, o § 1º do artigo 26 da LGPD elenca as hipóteses que permitirão este compartilhamento pelo Poder Público com entidades privadas:

> Art.26. O uso compartilhado de dados pessoais pelo Poder Público deve atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas.
> I - em casos de execução descentralizada de atividade pública que exija a transferência, exclusivamente para esse fim específico e determinado, observado o disposto na Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação)_II - (VETADO);
> III - nos casos em que os dados forem acessíveis publicamente, observadas as disposições desta Lei.
> IV - quando houver previsão legal ou a transferência for respaldada em contratos, convênios ou instrumentos congêneres; ou
> V - na hipótese de a transferência dos dados objetivar exclusivamente a prevenção de fraudes e irregularidades, ou proteger e resguardar a segurança e a integridade do titular dos dados, desde que vedado o tratamento para outras finalidades (BRASIL, 2018).

Com efeito, é possível o compartilhamento de dados pela Administração Pública também com entes privados quando relacionados a atividade pública descentralizada e exigir a transferência dos dados, devendo possuir um fim específico e determinado[6] (BOSTELMANN; MAFRA, 2021, p.145)

Ainda, poderão ser transferidos para entidades privadas dados pessoais que são disponibilizados publicamente - pode-se citar aqui as informações constantes do Portal Transparência de

[6] A título de exemplo, o INSS compartilha os dados de segurados com instituições financeiras pagadoras de benefício (que são os bancos por onde o cidadão recebe seu benefício) mediante contrato com cláusula de preservação de sigilo das informações. Os dados de segurados também podem ser compartilhados com instituições representativas mediante Acordos de Cooperação Técnica – ACT e/ou outro instrumento definido em lei (BRASIL, 2021).

cada órgão público - ou que deverão ser disponibilizados por cumprimento de obrigação legal ou disposição contratual (contratos, convênios, etc). (BOSTELMANN; MAFRA, 2021, p.145).

As últimas exceções que entrariam na supracitada transferência a pessoas jurídicas de direito privado quando houver previsão legal ou a transferência for respaldada em contratos, convênios ou instrumentos congêneres, bem como quando for necessária para prevenir fraudes e irregularidades, a manutenção da segurança pública e da integridade do titular de dados. Nessa situação não há falar de tratar os dados para outras finalidades, sendo estritamente vinculado ao contido na norma (BOSTELMANN; MAFRA, 2021, p.145).

Para tanto, cabe ao Poder Público o dever de informar à **A**utoridade Nacional de Proteção de Dados (ANPD) toda vez que ocorrer a comunicação ou o uso compartilhado de dados pessoais de pessoa jurídica de direito público a pessoa de direito privado (art.9º, LGPD).

2. A SEGURANÇA E O SIGILO DOS DADOS PESSOAIS NA LGPD

De acordo com o *princípio da segurança* (art.6º, VII, LGPD), os agentes de tratamento dos dados pessoais devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação e difusão, desde a fase de concepção do produto ou do serviço até a sua execução.

A LGPD dedica todo um capítulo às medidas de segurança técnicas e administrativas que deverão ser implementadas pelos agentes de tratamento para proteger os bancos de dados pessoais de acessos não autorizados. Tais medidas se tornam relevantes, sobretudo em um cenário no qual a invasão de bancos

de dados e posterior vazamento das informações ali presentes são cada vez mais corriqueiros (SOUZA, 2020, p. 420).

Nesse contexto, um aspecto importante no debate sobre a proteção dos dados pessoais é a compreensão do papel que desempenham os *agentes de tratamento* para garantir a segurança e o sigilo dos dados que estão sob seu controle. Muito se discute sobre como o sistema de proteção de dados deve garantir que o titular tenha controle sobre os seus dados. Para além do controle exercido pelo titular, é necessário analisar como os dados são tratados por terceiros e quais são os deveres que precisam ser observados para que a tutela dos dados não seja frustrada (SOUZA, 2020, p.415).

Os agentes de tratamento são os responsáveis pelo tratamento dos dados pessoais, sujeitos às regras da LGPD e à fiscalização da Autoridade Nacional de Proteção de Dados - ANPD, órgão responsável por elaborar as Políticas e Normas sobre proteção de Dados Pessoais no Brasil, fiscalizar a atuação das organizações no que se refere às políticas de proteção de dados e aplicar as sanções previstas na Lei.

De acordo com o Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado da ANPD (ANPD, 2021, p.7), o *controlador* é o agente responsável por tomar as principais decisões referentes ao tratamento de dados pessoais e por definir a finalidade deste tratamento. Na maioria das vezes, o controlador será uma pessoa jurídica**,** seja de direito privado ou de direito público[7].

Contudo, o tratamento não precisa ser realizado diretamente pelo controlador. Muito embora o controlador também

[7] É o que ocorre, por exemplo, com o Instituto Nacional do Seguro Social - INSS, que toma as principais decisões a respeito do armazenamento, da eliminação ou do compartilhamento de informações que integram o banco de dados pessoais que é gerido no âmbito da autarquia federal para a concessão e manutenção de benefícios. Os principais tratamentos de dados realizados pelo INSS estão relacionados à atualização de dados cadastrais, atualização e informações relativas a vínculos de trabalho, remunerações e contribuições e dados de dependentes. O tratamento das informações se destina, como regra, à concessão e manutenção de benefícios (BRASIL, 2021).

trate dados pessoais, o elemento distintivo é o poder de decisão, admitindo-se que o controlador forneça instruções para que um terceiro (operador) realize o tratamento em seu nome (art. 5º, VII; art. 39). (ANPD, 2021, p.10)

Nessa linha, *o operador* é o agente responsável por realizar o tratamento de dados em nome do controlador e conforme a finalidade por este delimitada. A definição legal se encontra no art. 5º, inciso X da LGPD[8] e implica dizer que o operador só poderá tratar os dados para a finalidade previamente estabelecida pelo controlador. Isso demonstra a principal diferença entre o controlador e operador, qual seja, o poder de decisão: o operador só pode agir no limite das finalidades determinadas pelo controlador.

De acordo com a LGPD, pessoas físicas e jurídicas de direito público e privado podem atuar como operadoras. Na maior parte das vezes, o operador é uma pessoa jurídica, que é contratada pelo controlador para realizar o tratamento de dados, conforme as instruções deste (ANPD, 2021, p.16)[9].

Além disso, conforme disposto no artigo 41 da LGPD, o controlador de dados deverá indicar um encarregado pelo tratamento de dados pessoais. O *encarregado* é o indivíduo responsável por garantir a conformidade de uma organização, pública ou privada, à LGPD. É o profissional que recebe as reclamações, faz os esclarecimentos e toma medidas necessárias, além de orientar os demais funcionários sobre as diretrizes da LGPD (ANPD, 2021, p. 22)[10]

Feitas essas considerações, cabe mencionar que o

[8] Nesse mesmo sentido é a previsão do art. 39 da LGPD: "O operador deverá realizar o tratamento segundo as instruções fornecidas pelo controlador, que verificará a observância das próprias instruções e das normas sobre a matéria".

[9] É o que ocorre, por exemplo, com a DATAPREV, que faz o tratamento dos dados do INSS para fins de concessão e manutenção de benefícios.

[10] O artigo 41 da LGPD não faz distinção quanto a instituições públicas ou privadas e por isso é importante que ambas estejam cientes da sua obrigação de indicar um encarregado de dados. A esse respeito, o art. 23, III, reforça a necessidade de um encarregado ser indicado por órgãos e entidades públicas (ANPD, 2021, p.22).

Capítulo VII da LGPD, cujo título é "Da segurança e das boas práticas", torna evidente, logo em seu artigo 46, a necessária adoção de medidas de segurança pelos agentes de tratamento acima mencionados

> Art. 46. Os agentes de tratamento devem adotar medidas de segurança, 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 qualquer forma de tratamento inadequado ou ilícito.

A partir do uso do imperativo do verbo "dever", verifica-se que a proteção adequada dos dados pessoais não é uma faculdade dos agentes de tratamento. Trata-se, na verdade, de uma imposição legal cujo descumprimento enseja a aplicação de sanções administrativas e eventual responsabilização civil (COTS; OLIVEIRA, 2018, p.150).

A LGPD apresenta ainda outra aplicação prática do princípio da segurança. De acordo com o art.44, o tratamento de dados pessoais é irregular quando não fornecer a segurança que o titular dele pode esperar. O artigo ainda estabelece algumas circunstâncias relevantes que devem ser observadas.

> Art. 44. O tratamento de dados pessoais será irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes, entre as quais:
> I - o modo pelo qual é realizado;
> II - o resultado e os riscos que razoavelmente dele se esperam;
> III - as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado.

Sobre o tema, ressalta-se que o Decreto 8.771/2016, que regulamenta o Marco Civil da Internet, detalha os padrões de segurança e sigilo dos registros, dados pessoais e comunicações privadas em seu Capítulo III. Na ausência de manifestação da Autoridade Nacional de Proteção de Dados, a doutrina defende que a redação do art.13 do Decreto poderá ser utilizada como parâmetro para os agentes de tratamento

> Art. 13. Os provedores de conexão e de aplicações devem, na guarda, armazenamento e tratamento de dados pessoais e

> comunicações privadas, observar as seguintes diretrizes sobre padrões de segurança:
> I - o estabelecimento de controle estrito sobre o acesso aos dados mediante a definição de responsabilidades das pessoas que terão possibilidade de acesso e de privilégios de acesso exclusivo para determinados usuários;
> II - a previsão de mecanismos de autenticação de acesso aos registros, usando, por exemplo, sistemas de autenticação dupla para assegurar a individualização do responsável pelo tratamento dos registros;
> III - a criação de inventário detalhado dos acessos aos registros de conexão e de acesso a aplicações, contendo o momento, a duração, a identidade do funcionário ou do responsável pelo acesso designado pela empresa e o arquivo acessado, inclusive para cumprimento do disposto no art. 11, § 3º, da Lei nº 12.965, de 2014; e
> IV - o uso de soluções de gestão dos registros por meio de técnicas que garantam a inviolabilidade dos dados, como encriptação ou medidas de proteção equivalentes (BRASIL, 2016).

Ademais, a norma da ABNT ISO/IEC 27002, conhecida como "Código de prática para a gestão da segurança da informação", também pode servir de subsídio aos agentes de tratamento, uma vez que dispõe sobre condutas e medidas para assegurar e preservar os dados sob sua administração (SOUZA, 2020, p.422).

No campo da segurança administrativa dos dados pessoais, é recomendado que o agente de tratamento desenvolva uma Política de Segurança de Informação (PSI), prescrevendo ações, proibições, boas práticas e até mesmo sanções. O PSI funciona como um código de conduta a ser seguido pelos funcionários e busca impedir o acesso daquelas informações por terceiros não autorizados (SOUZA, 2020, p.430-431).

O artigo 50 da LGPD, ao dispor sobre a possibilidade dos controladores e operadores adotarem regras de boas práticas e governanças, aponta o mínimo a ser seguido pelos agentes de tratamento ao implementar o programa de governança em privacidade (SOUZA, 2021, p.431).

Portanto, os agentes de tratamento e também qualquer

outra pessoa que intervenha em qualquer das fases de tratamento devem implementar padrões de segurança aptos a proteger os dados pessoais.

A noção de segurança e de sigilo devem assim permear todas as atividades de tratamento de dados, desde a concepção de um produto ou serviço. A noção de *privacy by design* é um ponto importante trazido pela LGPD e que merece destaque como um dos elementos mais relevantes do capítulo sobre segurança dos dados (SOUZA, 2020, p.422). Além disso, o art.48 da LGPD assenta a obrigação do controlador de comunicar à autoridade nacional a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.

Em caso de infrações decorrentes do descumprimento das regras impostas aos agentes de tratamento de dados – controlador e operador -, estes estarão sujeitos a penalidades administrativas elencadas no art.52 da LGPD, aplicáveis pela Autoridade Nacional de Proteção de Dados - ANPD, após procedimento administrativo que garantirá a ampla defesa ao agente, e utilizará como como parâmetro a gravidade e a natureza das infrações e dos direitos pessoais afetados; a boa-fé do infrator; a vantagem auferida ou pretendida pelo infrator; a condição econômica do infrator; a reincidência; o grau do dano; a cooperação do infrator; a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados, a adoção de política de boas práticas e governança; a pronta adoção de medidas corretivas; e a proporcionalidade entre a gravidade da falta e a intensidade da sanção.

As punições decorrentes de infrações às normas de proteção de dados previstas na lei correspondem a advertência, multa simples e multa diária, publicização da infração, bloqueio e eliminação dos dados pessoais em questão (art.52, da LGPD).

A LGPD traz ainda seção específica de responsabilidade para o Poder Público nos artigos 31 e 32 que tratam de medidas

administrativas a serem tomadas para os casos de infração da lei ou para o monitoramento de adoção de boas práticas.

Recentemente a Agência Nacional de Proteção de Dados excluiu a possibilidade de que as sanções pecuniárias, previstas no artigo 52, possam ser aplicadas a órgãos públicos. Estas medidas não afastam a incidência das normas do artigo 42 e 43 da Lei para o Poder Público, com as devidas adaptações decorrentes da responsabilidade objetiva do Estado (SIMÕES, 2021, n.p.).

Outrossim, instrumento importante para estimular a aplicação dos dispositivos da lei em caráter preventivo, e demonstrar seu compromisso com a efetividade das normas atinentes à proteção de dados, é a responsabilização pelo descumprimento das normas da LGPD e o consequente ressarcimento de eventuais danos causados aos titulares por compartilhamentos, transferências e vazamentos de dados pessoais estão elencados nos artigos 42 a 45 da LGPD e serão analisados a seguir.

3. O REGIME DE RESPONSABILIZAÇÃO CIVIL NA LGPD

O dispositivo da LGPD que regula a responsabilidade civil pela violação das regras atinentes à atividade de tratamento de dados pessoais é o artigo 42

> Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo (BRASIL, 2018).

Tal dispositivo encontra respaldo em regras elementares de responsabilidade civil, principalmente no caput do art.927 do Código Civil, a estabelecer que "aquele que, por ato ilícito causar dano a outrem, fica obrigado a repará-lo".

Contudo, a legislação não é clara com relação a espécie de responsabilidade. Assim, desde sua entrada em vigor, discute-se na doutrina e na jurisprudência se a responsabilidade prevista na Lei será objetiva, subjetiva ou ainda uma terceira

hipótese, a objetiva especial. Da mesma forma, a LGPD não definiu como será o regime de responsabilização específica para a Administração Pública.

Bruna Simões (2021, n.p.) explica que os defensores da responsabilidade objetiva argumentam que a lei trouxe grandes semelhanças com o Código de Defesa do Consumidor, inclusive com a redação do artigo 43 trazendo as hipóteses de excludente de responsabilidade. Com efeito, a responsabilidade se daria em razão do risco ou proveito da atividade. Já os defensores da responsabilidade subjetiva entendem que a sistemática de Lei, estabelecendo normas de conduta para o tratamento de dados é típica da responsabilidade subjetiva e depende da comprovação de culpa dos agentes de tratamento de dados. Para a terceira corrente, que chama a responsabilidade de objetiva especial, ela decorre do cometimento de um ilícito pelos agentes do tratamento de dados, ou seja, pelo descumprimento dos deveres previstos na lei, em especial o de segurança.

Realizando uma interpretação sistemática, histórica e gramatical da LGPD, levando em consideração o sistema em que ela está inserida, os fatos históricos que antecederam a norma e o processo legislativo de sua criação, bem como a análise individual e contextual dos termos do texto legal, tendo por base as regras da linguística, buscar-se-á avaliar qual o regime de responsabilização fixado pela lei.

Do ponto de vista sistemático, a primeira constatação que decorre da LGPD é que o regime de responsabilização por ela estabelecido exige a análise qualitativa da conduta do agente no tratamento de dados para que surja a obrigação de indenizar os danos causados aos seus titulares. Isso decorre da interpretação textual do 44 da LGPD, quando diz que "o tratamento de dados pessoais será irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes", dentre os quais:

> I - o modo pelo qual é realizado;
>
> II - o resultado e os riscos que razoavelmente dele se esperam;

> III - as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado.
> Parágrafo único. Responde pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no art. 46 desta Lei, der causa ao dano (BRASIL, 2018).

Com efeito, caso o legislador tivesse optado pela responsabilidade objetiva, não teria previsto na LGPD uma série de condutas específicas a serem seguidas no tratamento de dados pelo agente (CORRÊA; CHO, 2021, n.p.).

Nesse mesmo sentido, Gustavo Tepedino, Aline de Miranda Terra e Gisela Sampaio da Cruz Guedes (2020, p. 236-252) defendem a responsabilidade subjetiva, sob o argumento de que a lógica da responsabilidade objetiva é outra. Nela, não cabe discutir cumprimento de deveres, porque a responsabilidade objetiva não decorre do descumprimento de qualquer dever jurídico. Quando se discute cumprimento de deveres, o que no fundo está sendo analisado é se o agente atuou ou não com culpa.

> *Assim, apesar de a LGPD não ser explícita em relação à natureza da responsabilidade dos agentes de tratamento de dados, como é o Código de Defesa do Consumidor ao adotar a responsabilidade objetiva, a interpretação sistemática da LGPD leva à conclusão de que o regime adotado por este diploma foi mesmo o da responsabilidade subjetiva.*
> *Não obstante as semelhanças com o Código de Defesa do Consumidor, é essencial destacar que, enquanto o Código de Defesa do Consumidor tem pelo menos dois artigos expressamente indicando a natureza objetiva da responsabilidade (arts. 12 e 14 – ambos se valem da expressão "independentemente de culpa", que deixa clara a opção do legislador pela responsabilidade objetiva), não há qualquer norma análoga na LGPD. O art. 42 da LGPD não faz referência expressa à culpa como elemento da responsabilidade civil, mas também não faz qualquer alusão ao risco como fundamento da responsabilidade objetiva"* (TEPEDINO; TERRA; GUEDES, 2020, p. 236-252).

Do ponto de vista histórico, uma segunda constatação é que o dispositivo da LGPD que remetia para a responsabilidade

objetiva foi retirado do texto final durante o trâmite legislativo, o que é um dado significativo para a interpretação da lei. Portanto, "o próprio histórico de tramitação do projeto de lei que deu origem à LGPD evidencia, portanto, a opção do legislador pela responsabilidade subjetiva" (TEPEDINO; TERRA; GUEDES, 2020, p. 236-252).

Do ponto de vista gramatical, uma terceira constatação é que a lei prevê excludentes de responsabilidade, devidamente tutelada em três hipóteses do artigo 43:

> Art. 43. Os agentes de tratamento só não serão responsabilizados quando provarem:
> I - que não realizaram o tratamento de dados pessoais que lhes é atribuído;
> II - que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou
> III - que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro.

Em suma, extrai-se do texto legal que não basta o mero desempenho da atividade de tratamento de dados para que seja possível imputar responsabilidade ao agente. É necessário um comportamento culposo, seja por violar diretamente a legislação de proteção de dados (artigo 42), seja por deixar de tomar medida(s) de segurança adequada(s) (artigo 44) (CORRÊA; CHAO, 2021, n.p.).

Nesse ponto, destaca-se a posição defendida por Maristrello Porto (2019, p.180) que demonstra, sob a ótica da análise econômica do Direito[11], que ″determinada regra de responsabilização é desejável se fornece os incentivos adequados para que os agentes adotem níveis adequados de precaução no exercício

[11] A Análise Econômica do Direito, conhecida também como Law & Economics ou Direito e Economia, é definida como "a aplicação da teoria e de métodos econométricos no exame da formação, estrutura, processos e impacto do Direito e das instituições jurídicas" (BATTESINI, 2011, p. 25). É um método pelo qual se permite avaliar se o emprego de determinada regra ou política pública causará os efeitos que dela se esperam. Procura, portanto, auxiliar na tomada de decisões jurídicas ao considerar custos e benefícios e outros critérios de eficiência econômica e social (CARDOSO, 2019).

de suas atividades″. Isso porque:

> A responsabilidade protege os direitos exclusivos sobre bens escassos, procura desencorajar danos, internalizar as externalidades e, assim, impor que todos suportem o custo integral de seu comportamento.
>
> O instituto serve, ao mesmo tempo, para indenizar a vítima. Esse objetivo não pode, porém, ser o único a informar a responsabilidade civil extracontratual, pois o risco seria deslizar para a lógica do "deep pocket" (responsabilidade medida pela solvabilidade do réu). Esse escorregão pode aumentar, sem limites, os custos derivados de acidentes e à sua prevenção (PORTO, 2019, p.180).

Com efeito, "se o cumprimento dos deveres não levasse a alguma mudança nos parâmetros para a responsabilização, não haveria incentivo para o seu cumprimento" (CORRÊA; CHO, 2021).

Portanto, a partir de uma interpretação sistemática, histórica e gramatical, a conclusão é no sentido de que a responsabilidade prevista na LGPD é subjetiva, ou seja, assim como o dano, o nexo de causalidade e o ato ilícito, a culpa genérica também é elemento essencial para configurar o dever de indenizar.

A partir dessa constatação, debate-se na doutrina e na jurisprudência qual seria a espécie de responsabilidade civil do Estado por violação da LGPD, tendo em vista a responsabilidade subjetiva prevista na LGPD e a ausência de previsão de responsabilização específica para a Administração Pública.

A primeira vista, conforme exposto por Sthéfano Divino e Taisa de Lima (2020, p.17), depreende-se que "como a responsabilidade objetiva advém de uma prescrição legal, não podendo sê-la subentendida ou presumida, a princípio parece que, neste caso, deverá ser aplicada sua modalidade subjetiva". Com efeito, deveria verificar se houve participação de culpa no ato do poder público que eventualmente causou danos ao titular dos dados para a sua responsabilização.

Contudo, a questão se torna mais complexa, tendo em vista que existe a previsão geral da responsabilidade civil

objetiva do Estado fundada no art. 37, §6º, da CF/88[12], existindo doutrina no sentido de que essa discussão para a responsabilidade civil do Estado é despicienda em face da norma constitucional (SIMÕES, 2021, n.p.). Para essa corrente, fixada a responsabilidade objetiva para o ente estatal, basta a verificação do nexo causal para que seja devida a indenização ela exposição indevida de dados.

A dificuldade encontrada neste ponto é que nas operações que envolvem transmissões de dados, nem sempre é possível demonstrar a origem do vazamento, dificultando a comprovação do nexo causal (SIMÕES, 2020, n.p.). Para a solução de tal problema, vem se indicando a aplicação da inversão do ônus da prova a critério do juiz, a favor do titular de dados, desde que verossímil a alegação, haja hipossuficiência para fins de produção de prova ou quando a produção de prova pelo titular for excessivamente onerosa.

Dessa forma, no tocante a responsabilização da Administração Pública pelo descumprimento dos deveres impostos pela LGPD, a pouca doutrina e jurisprudência existentes sobre o tema ainda se encontram divididas entre a necessidade de comprovação da culpa genérica (responsabilidade subjetiva), nos termos da regra geral da LGPD ou a aplicação da responsabilidade objetiva, independentemente de culpa, por omissão específica, com fulcro no art. 37, § 6º, da CF e na interpretação do STF a respeito do tema.

Por fim, cumpre frisar que, embora a LGPD não traga parâmetros de indenização em caso de responsabilidade civil, com base no artigo 944 do Código Civil, pode-se ter em consideração critérios estabelecidos na própria lei como relevantes para fixação do dano, especialmente aqueles dispostos no §1º do artigo 52, tais como a sensibilidade dos dados, a reincidência do

[12] Art. 37, §6º: As pessoas jurídicas de direito público e as de direito privado prestadoras de serviços pública responderão pelos danos que seus agentes, nessa qualidade, causarem a terceiros, assegurado o direito de regresso contra o responsável nos casos de dolo ou culpa (BRASIL, 1988).

agente e a ausência ou demora na notificação do vazamento de dados[13].

CONSIDERAÇÕES FINAIS

A LGPD disciplinou o tratamento de dados pessoais não apenas pelos entes privados, mas também pelas pessoas jurídicas de direito público, tendo em vista que o Poder Público é um dos maiores interessados na coleta de dados pessoais, o que exige dos titulares a exposição de suas informações pessoais para fins de execução de atividades administrativas e de implementação de políticas públicas.

Considerando que a proteção de dados corresponde a verdadeiro direito fundamental autônomo, expressão da liberdade e da dignidade humana, agora previsto no art.5º, inciso LXXIX, da Constituição, está intrinsecamente relacionada à impossibilidade de transformar os indivíduos em objeto de vigilância.

Nesse contexto, ao dispor sobre o tratamento de dados, a LGPD prevê, em seu art.7º, as hipóteses legais taxativas que autorizam o tratamento de dados pessoais. Tratando-se da Administração Pública, a LGPD permite o tratamento e o compartilhamento de dados pessoais, independente do consentimento do titular, para execução de políticas públicas, previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres.

Conforme restou demonstrado, o compartilhamento de dados pessoais pelo Poder Público é permitido entre os órgãos públicos e só poderá ser concedido quando os dados tratados forem necessários para elaboração de políticas públicas ou quando houver determinação legal para tanto. Contudo, ainda que a

[13] Nesse sentido, como colocado por Nelson Rosenvald (2021, on line), para a análise da extensão do dano e considerando a previsão do artigo 50 da Lei 13.709/18 sobre adoção de boas práticas e de governança, deve-se considerar a diligência ou o *standard* adotado pelo órgão a ser condenado.

regra geral seja de que o Poder Público não possa transferir às empresas privadas os dados pessoais armazenados em seus bancos de dados, o § 1º do artigo 26 da LGPD elenca as hipóteses que permitirão, excepcionalmente, este compartilhamento.

Na sequência, esclareceu-se que a LGPD dedica todo um capítulo às medidas de segurança técnicas e administrativas que deverão ser implementadas pelos agentes de tratamento para proteger os bancos de dados pessoais de acessos não autorizados. Em caso de infrações decorrentes do descumprimento das regras impostas aos agentes de tratamento de dados – controlador e operador -, estes estarão sujeitos a penalidades administrativas e civis.

Não obstante o silêncio da lei, a doutrina majoritária vem entendendo, a partir de uma interpretação sistemática, histórica e gramatical, que a responsabilidade prevista na LGPD é subjetiva, ou seja, assim como o dano, o nexo de causalidade e o ato ilícito, a culpa genérica também é elemento essencial para configurar o dever de indenizar.

Nesse ponto, em que pese a LGPD estabelecer a regra geral da responsabilidade subjetiva, no que toca ao regime de responsabilização da Administração Pública, a doutrina e a jurisprudência estão divididas entre a necessidade de comprovação da culpa genérica (responsabilidade subjetiva) ou a aplicação da responsabilidade objetiva, independentemente de culpa, tendo em vista a previsão do art. 37, § 6º, da CF. Para a corrente que defende a responsabilidade objetiva do Poder Público, basta a verificação do nexo causal para que seja devida a indenização pela exposição indevida de dados.

Por fim, restou esclarecido que embora a LGPD não traga parâmetros de indenização em caso de responsabilidade civil, com base no artigo 944 do Código Civil, pode-se ter em consideração critérios estabelecidos na própria lei como relevantes para fixação do dano, especialmente aqueles dispostos no §1º do artigo 52, tais como a sensibilidade dos dados, a reincidência do

agente e a ausência ou demora na notificação do vazamento de dados.

REFERÊNCIAS

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS - ANPD. *Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado*. Brasília, DF, maio de 2021. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-publica-guia-orientativo-sobre-agentes-de-tratamento-e-encarregado Acesso em: 15 dez. 2021

BATTESINI, Eugênio. *Direito e Economia*: novos horizontes da responsabilidade civil no Brasil. São Paulo: LTr, 2011.

BOMFIM, Gilberto; CASTRO, Bruno Fediuk de. A quarta revolução industrial e seus impactos nos direitos fundamentais à privacidade e proteção de dados. In: *Law Experience - Direitos Fundamentais na era Tecnológica*. Organização Miriam Olivia Knopik Ferraz, Karlo Messa Vettorazi. 1.a ed. Curitiba: FAE/Bom Jesus, 2020. p.65-78.

BRASIL. *Constituição da República Federativa do Brasil***.** Brasília, DF: Câmara dos Deputados, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm Acesso em: 17 mar. 2022.

BRASIL. *Decreto nº 8.771, de 11 de maio de 2016*. Regulamenta a Lei nº 12.965, de 23 de abril de 2014, para tratar das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de

transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações. Brasília, DF: Câmara dos Deputados.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. *Lei Geral de Proteção de Dados Pessoais (LGPD).* Brasília, DF: Câmara dos Deputados, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 15 dez. 2021.

BRASIL. Ministério do Trabalho e Previdência. Instituto Nacional do Seguro Social. *Lei Geral de Proteção de Dados Pessoais (LGPD).* Brasília, DF: 2021. Disponível em: https://www.gov.br/inss/pt-br/acesso-a-informacao/lei-geral-de-protecao-de-dados-pessoais Acesso em: 15 dez. 2021.

BOSTEMANN, Danielle Santi; MAFRA, Marcos Guilherme Rodrigues. *A responsabilidade da Administração Pública na Lei Geral de Proteção de Dados*. In: PIRONTI, Rodrigo (Coord.). Lei Geral de Proteção de Dados no Setor Público. Belo Horizonte: Fórum, 2021. p.137-150. ISBN 978-65-5518-141-8.

CORRÊA, Leonardo; CHO, Tae. Responsabilidade civil na LGPD é subjetiva. São Paulo: *Revista Consultor Jurídico*, 2021. Disponível em: https://www.conjur.com.br/2021-jan-29/correa-cho-responsabilidade-civil-lgpd-subjetiva. Acesso em: 15 dez. 2021. ISSN 1809-2829

COTS, Márcio; OLIVEIRA, Ricardo. *Lei Geral de Proteção de Dados Pessoais (LGPD) comentada.* São Paulo: Ed. RT, 2018.

DIVINO, Sthéfano Bruno Santos; LIMA, Taisa Maria Macena de. RESPONSABILIDADE CIVIL NA LEI GERAL DE PROTEÇÃO DE DADOS BRASILEIRA. *Revista Em Tempo*, [S.l.], v. 20, n. 1, nov. 2020. ISSN 1984-7858.

Disponível em: <https://revista.univem.edu.br/emtempo/article/view/3229>. Acesso em: 25 jan. 2022. doi: https://doi.org/10.26729/et.v20i1.3229.

DONEDA, Danilo Cesar Maganhoto. *Da privacidade à proteção de dados pessoais* [livro eletrônico]: elementos da formação da Lei Geral de Proteção de Dados. 2. ed. -- São Paulo: Thomson Reuters Brasil, 2020. ISBN 978-65-5065-030-8

FRAZÃO, Ana. Objetivos e alcance da Lei Geral de Proteção de Dados. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coord.). *Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro*. 2a. Ed. São Paulo: Thompson Reuters Brasil, 2020. p.479-497.

PIRONTI, Rodrigo; ZILIOTTO, Mirela Miró. *O direito à autodeterminação informativa e a questão do consentimento no tratamento de dados pessoais***.** In: PIRONTI, Rodrigo (Coord.). Lei Geral de Proteção de Dados no Setor Público. Belo Horizonte: Fórum, 2021. p.407-426. ISBN 978-65-5518-141-8.

PORTO, Antônio José Maristello. Análise Econômica da Responsabilidade Civil. In: *Direito e Economia no Brasil* - Estudos sobre a análise econômica do direito - 3a Ed. Cidade Nova: Editora Foco, 2019. p.180-200

ROSENVALD, Nelson. O compliance e a redução equitativa da indenização na LGPD. *Revista Migalhas*. 10 de março de 2021. https://www.migalhas.com.br/coluna/migalhas-de-protecao-de-dados/342032/o-compliance-e-a-reducao-equitativa-da-indenizacao-na-lgpd Acesso em: 28 mar. 2022.

SIMÕES, Bruna. LGPD e a responsabilidade civil do Estado. *Revista Migalhas*. 26 de agosto de 2021. Disponível em: https://www.migalhas.com.br/coluna/migalhas-de-responsabilidade-civil/350717/lgpd-e-a-responsabilidade-

civil-do-estado Acesso em: 17 mar. 2022.

SOUZA, Carlos Affonso Pereira de. Segurança e sigilo dos dados pessoais: primeiras impressões à luz da Lei 13.709/2018. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coord.). *Lei Geral de Proteção de Dados Pessoais e suas repercusões no Direito Brasileiro*. 2a. Ed. São Paulo: Thompson Reuters Brasil, 2020. p.413-437.

TEPEDINO, Gustavo, TEFFÉ, Chiara Spadaccini de. Consentimento e proteção de dados pessoais na LGPD. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coord.). *Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro*. 2a. Ed. São Paulo: Thompson Reuters Brasil, 2020. p.281-3187.

TEPEDINO, Gustavo; TERRA, Aline de Miranda; GUEDES, Gisela Sampaio da Cruz. *Fundamentos de Direito Civil: Responsabilidade* Civil. Vol.4, 2a Ed. Forense: São Paulo, 2020.

UNIÃO EUROPEIA, Agência dos Direitos Fundamentais. *Manual da Legislação Europeia sobre Proteção de Dados*. Luxemburgo: Serviço das Publicações da União Europeia, 2014, p. 39. Disponível em: https://rm.coe.int/16806ae65f. Acesso em: 11 abr. 2019.

XAVIER, Luciana Pedroso; XAVIER, Marília Pedroso; SPALER, Mayara Guibor. Primeiras impressões sobre o tratamento de dados pessoais nas hipóteses de interesse público e execução de contratos. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coord.). *Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro*. 2a. Ed. São Paulo: Thompson Reuters Brasil, 2020. p.479-497.