

UNIVERSIDADE PRESBITERIANA MACKENZIE

PEDRO CÉSAR SOARES DE MACEDO BURIM

RESPONSABILIDADE CIVIL DO ESTADO POR DANOS CAUSADOS AO TITULAR
DE DADOS PESSOAIS SEGUNDO A LGPD

São Paulo

2022

PEDRO CÉSAR SOARES DE MACEDO BURIM

RESPONSABILIDADE CIVIL DO ESTADO POR DANOS CAUSADOS AO TITULAR
DE DADOS PESSOAIS SEGUNDO A LGPD

Trabalho de Conclusão de Curso apresentado à banca examinadora da Universidade Presbiteriana Mackenzie, como exigência parcial para a obtenção do grau de bacharel em Direito.

ORIENTADORA: Prof^a Denise Neves Abade

São Paulo

2022

Burim, Pedro César Soares de Macedo

Responsabilidade civil do Estado por danos causados ao titular de dados pessoais segundo a LGPD

60f. il.:

Orientador: Prof^ª Denise Abade

Monografia (Curso de Graduação em Direito) Campus Higienópolis
Universidade Presbiteriana Mackenzie, São Paulo, 2022.

1. Proteção de dados pessoais no Brasil 2. Tratamento dos dados pessoais 3. Atividade estatal e o sistema de proteção de dados 4. Responsabilidade civil do Estado pelo indevido manejo de dados pessoais. I. Abade, Denise. II Universidade Presbiteriana Mackenzie. Faculdade de Direito III. Título.

PEDRO CÉSAR SOARES DE MACEDO BURIM

RESPONSABILIDADE CIVIL DO ESTADO POR DANOS CAUSADOS AO TITULAR
DE DADOS PESSOAIS SEGUNDO A LGPD

Trabalho de Conclusão de Curso apresentado à banca examinadora da Universidade Presbiteriana Mackenzie como requisito parcial para obtenção do grau de bacharel em Direito.

Aprovado em

BANCA EXAMINADORA

Prof.^a Denise Neves Abade

Universidade Presbiteriana Mackenzie

Prof.^a Andréia Regina Schneider Nunes Carvalhaes

Universidade Presbiteriana Mackenzie

Prof.^a Mariana Barboza Baeta Neves Matsushita

Universidade Presbiteriana Mackenzie

RESUMO

O presente trabalho de conclusão de curso tem o objetivo de discutir se é possível aplicar a responsabilização civil ao Estado pelo indevido manejo de dados pessoais do titular, conforme a Lei Geral de Proteção de Dados. O estudo foi realizado através dos métodos teórico e qualitativo, utilizando-se como fontes de pesquisa livros, artigos científicos, teses, dissertações, a lei e a jurisprudência brasileira. Após discorrer sobre o sistema de proteção de dados e o surgimento da Lei Geral de Proteção de Dados no Brasil, o tratamento de dados pessoais pelos controladores e operadores, os pressupostos da responsabilidade civil e a aplicação desta ao Poder Público, chegou-se à conclusão de que é possível aplicar a responsabilização civil pelo uso indevido de dados pessoais ao Poder Público, em consonância com a Lei Geral de Proteção de Dados e o ordenamento jurídico brasileiro.

Palavras-chave: Dados Pessoais. Direito Administrativo. Responsabilidade Civil. Lei Geral de Proteção de Dados Pessoais. Poder Público.

ABSTRACT

The present end-of-course paper aims to discuss whether it is possible to apply civil liability of the State for the improper handling of the holder's personal data, according to the General Law of Data Protection. The study was carried out through theoretical and qualitative methods, using as research sources books, scientific articles, theses, dissertations, the law and Brazilian case law. After discussing the data protection system and the emergence of the General Law of Data Protection in Brazil, the treatment of personal data by controllers and operators, the assumptions of civil liability and its application to the Public Power, the conclusion was reached that it is possible to apply civil liability for the misuse of personal data to the Public Power, in accordance with the General Law of Data Protection and the Brazilian legal system.

Keywords: Personal Data. Administrative Law. Civil Liability. General Law of Personal Data Protection. Public Power.

SUMÁRIO

INTRODUÇÃO	6
1. PROTEÇÃO AOS DADOS PESSOAIS NO BRASIL	8
1.1 DIREITO À PRIVACIDADE E A PROTEÇÃO AOS DADOS PESSOAIS	8
1.2 A PROTEÇÃO AOS DADOS PESSOAIS NO BRASIL ANTES DO SURGIMENTO DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS	10
1.3 ASPECTOS GERAIS SOBRE A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS	15
2. TRATAMENTO DOS DADOS PESSOAIS	24
2.1 AGENTES DE TRATAMENTO DE DADOS E SUAS OBRIGAÇÕES	24
2.2 TIPOS DE DADOS SEGUNDO A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS	26
2.3 TÉRMINO DO TRATAMENTO DE DADOS	28
2.4 OS DIREITOS DO TITULAR DE DADOS	30
3. ATIVIDADE ESTATAL E O SISTEMA DE PROTEÇÃO DE DADOS	38
3.1 TRATAMENTO DOS DADOS PESSOAIS PELO PODER PÚBLICO	38
3.2 PROTEÇÃO AOS DADOS PESSOAIS <i>VERSUS</i> INTERESSE PÚBLICO	44
4. RESPONSABILIDADE CIVIL DO ESTADO PELO INDEVIDO MANEJO DE DADOS PESSOAIS	46
4.1 ASPECTOS GERAIS E PRESSUPOSTOS DA RESPONSABILIDADE CIVIL	46
4.2 RESPONSABILIDADE CIVIL DO ESTADO E TEORIA DO RISCO ADMINISTRATIVO	52
4.3 RESPONSABILIDADE CIVIL DO ESTADO PELOS DANOS CAUSADOS POR SEUS AGENTES ATRAVÉS DO INDEVIDO MANEJO DE DADOS PESSOAIS SEGUNDO A LGPD	54
CONCLUSÃO	59
REFERÊNCIAS	61

INTRODUÇÃO

Com a explosão da era da informação e o crescimento do mundo digital, o Direito passou a preocupar-se cada vez mais com a proteção dos dados pessoais, culminando na promulgação da Lei Geral de Proteção de Dados Pessoais no Brasil, no ano de 2018.

A referida lei buscou proteger um dos principais direitos da personalidade humana, consagrado na Constituição Federal e no Código Civil: o direito à privacidade, através do estabelecimento de princípios, definições e regras sobre os direitos e deveres da relação jurídica que interliga os controladores e operadores de dados com os titulares de tais informações no momento do tratamento de dados pessoais.

A referida lei, de idade relativamente nova, passou a determinar, também, em quais situações o indivíduo responsável pelo tratamento dos dados viola os direitos do titular destes, passando a prever hipóteses de responsabilização civil àqueles que causarem danos em virtude do indevido manejo dos dados pessoais alheios.

Diante do exposto, surge o seguinte questionamento: a hipótese de responsabilidade civil por uso indevido de dados, disposta na LGPD, aplica-se ao Estado? A pergunta é interessante, tendo em vista o forte desequilíbrio da relação deste com o particular, o qual acaba ficando muitas vezes subordinado à vontade estatal, e pode ser tolhido de certos direitos quando, por exemplo, buscando proteger sua privacidade, negar-se a fornecer seus dados pessoais à Administração Pública, como será explorado no decorrer deste estudo.

Nesse contexto, a aplicação da responsabilização civil do Estado pelo manejo indevido de dados pessoais de terceiros se demonstra possível diante de uma análise sistemática da Lei Geral de Proteção de Dados Pessoais, que em alguns de seus artigos, disciplina o tratamento de dados pessoais pelo Poder Público, submetendo este, portanto às suas regras.

Portanto, o objetivo geral do presente trabalho é estudar a Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito brasileiro, passando pelo Direito Administrativo e pelo instituto da responsabilidade civil, de forma que o objetivo específico é o de demonstrar que a responsabilidade civil por uso indevido de dados pessoais alheios é plenamente aplicável ao Poder Público.

A vulnerabilidade da relação do administrado com a Administração Pública e o indevido uso de dados pessoais alheios pelo ente estatal afetam milhões de brasileiros. Sendo assim, fica evidente que a solução apresentada neste estudo, favorável à responsabilidade civil estatal em

razão de ilícitos cometidos quanto ao manejo de dados pessoais do particular impacta uma grande parcela da sociedade brasileira.

O presente trabalho foi desenvolvido com base nos métodos teórico e qualitativo, através das mais variadas fontes de pesquisa, tais quais livros, artigos científicos, teses, dissertações, leis e a jurisprudência brasileira.

A pesquisa foi dividida em quatro capítulos. No primeiro capítulo, foram trazidos aspectos gerais sobre a proteção dos dados pessoais no Brasil, estabelecendo-se a relação entre a proteção ao direito à privacidade e a proteção de dados pessoais, e retratando como esta se deu antes do surgimento da LGPD, que teve, ao final do capítulo, seus aspectos gerais retratados.

Na sequência, o segundo capítulo adentrou nas disposições da LGPD, trazendo aspectos sobre os agentes envolvidos no tratamento de dados pessoais e suas obrigações, os tipos de dados pessoais existentes, o término do tratamento de dados e os direitos do titular de dados na referida lei.

Já no terceiro capítulo, foram estudadas a atividade estatal e sua atuação no tratamento de dados pessoais, sendo que, comentou-se, em primeiro lugar, sobre os principais aspectos acerca da Administração Pública e os princípios a ela aplicáveis, em segundo lugar, acerca do tratamento de dados pessoais pelo Poder Público e, por último, sobre o embate entre o interesse público e a proteção de dados pessoais.

Por fim, no quarto e derradeiro capítulo, foram estudados o instituto da responsabilidade civil e a responsabilidade civil estatal, defendendo-se, ao final, sua aplicação quando o Estado usa indevidamente dados pessoais alheios.

1. PROTEÇÃO AOS DADOS PESSOAIS NO BRASIL

1.1 DIREITO À PRIVACIDADE E A PROTEÇÃO AOS DADOS PESSOAIS

Não há como tratar sobre o direito à privacidade sem mencionar a proteção dada a este pela Constituição Federal, norma máxima do ordenamento jurídico brasileiro.

Nesse sentido, os incisos X e XII, do artigo 5º da norma maior, colocaram o direito à vida privada e o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas como invioláveis, no momento em que os elevou ao rol dos direitos fundamentais:

Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:

(...)

X - são invioláveis a intimidade, a **vida privada**, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação (**grifo nosso**);

(...)

XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, **de dados** e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal (**grifo nosso**) ;

Trazida a proteção constitucional, passa a ser primordial entender em que consiste o direito à privacidade.

Em um sentido mais amplo, Luiz Alberto David Araújo e Vidal Serrano Nunes Júnior (2016) estabelecem o seguinte:

Por privacidade, de conseguinte, devem-se entender os níveis de relacionamento social que o indivíduo habitualmente mantém oculto ao público em geral, dentre eles: a vida familiar, as aventuras amorosas, o lazer e o segredo dos negócios. Assim, dentro dessa esfera teríamos demarcado o território próprio da privacidade, formado por relações marcadas pela confidencialidade. (ARAÚJO; NUNES JÚNIOR, 2016, p. 200)

Por sua vez, André Carvalho de Ramos (2017, p. 702-703) assevera que “o direito à privacidade é um direito fundamental que permite que seu titular impeça que determinados

aspectos de sua vida sejam submetidos, contra a sua vontade, à publicidade e a outras turbações feitas por terceiros.”.

Dentro desses aspectos de vida que podem ser protegidos pelo titular do direito à privacidade, certamente estão inseridos os dados pessoais, os quais poderão ser protegidos por quem os detém, posto que fazem parte da exteriorização de sua personalidade, como será explanado a seguir.

Inspirado no dispositivo constitucional supracitado, o Código Civil de 2002, em seu artigo 21, inseriu o direito à vida privada no grupo dos direitos da personalidade (artigos 11 a 21), tratando-o como inviolável e abrindo a possibilidade de o interessado requerer em juízo a adoção das providências necessárias para impedir ou fazer cessar as condutas que o desrespeitarem.

Sendo a privacidade uma das espécies do gênero “direitos da personalidade”, certamente, ambos os institutos compartilham características entre si. Por tal razão, torna-se importante esclarecer o conceito e as características dos direitos da personalidade.

Nas palavras de Pablo Stolze Gagliano e Rodolfo Pamplona Filho, os direitos da personalidade podem ser conceituados da seguinte maneira:

Conceituam-se os direitos da personalidade como aqueles que têm por objeto os atributos físicos, psíquicos e morais da pessoa em si e em suas projeções sociais. A ideia a nortear a disciplina dos direitos da personalidade é a de uma esfera extrapatrimonial do indivíduo, em que o sujeito tem reconhecidamente tutelada pela ordem jurídica uma série indeterminada de valores não redutíveis pecuniariamente, como a vida, a integridade física, a intimidade, a honra, entre outros. (GAGLIANO; PAMPLONA FILHO, 2019, p. 235)

Dentre as principais características dos direitos da personalidade, Gagliano e Pamplona Filho (2019) destacam seu caráter absoluto (produzem efeitos em todos os campos e impõem à coletividade o dever de respeitá-los); a generalidade (outorgados a todos por sua existência); a extrapatrimonialidade (não têm conteúdo patrimonial direto, mas sua lesão pode gerar efeitos econômicos); a indisponibilidade (ligada à impossibilidade de o titular transmiti-los ou a eles renunciar); imprescritibilidade (não extinção em razão do não exercício); impenhorabilidade (não suscetíveis de penhora) e, por fim, a vitaliciedade (acompanham o titular do nascimento até a morte).

Apesar de os direitos da personalidade serem, em regra, irrenunciáveis, Ellen Carina Mattias Sartori (2016) admite que, em algumas situações, pode haver disponibilidade relativa sobre eles, como, por exemplo, quanto ao direito à privacidade, na cessão de dados pessoais em troca de acesso gratuito a algum serviço da internet. Segundo ela, esse fornecimento é possível,

desde que não seja vitalício, nem ilimitado, e que possa ser encerrado pelo titular dos dados a qualquer momento, sem necessidade de justificativas.

Ainda de acordo com Sartori (2016), a inviolabilidade à vida privada é a garantia ao indivíduo de autonomia quanto a quais de seus dados podem ser divulgados e quais não, e a relevância da proteção jurídica dos dados pessoais reside no fato de que estes são a extensão da personalidade de seu titular, concluindo que, por tal razão, a proteção aos dados pessoais nada mais é do que a proteção à personalidade.

Diante do que foi trazido, está demonstrada a grande relevância jurídica que a proteção aos dados pessoais possui, eis que, como visto, protegendo-os, acabam sendo resguardados, por consequência, o direito fundamental à vida privada, o qual é um dos mais importantes direitos da personalidade.

1.2 A PROTEÇÃO AOS DADOS PESSOAIS NO BRASIL ANTES DO SURGIMENTO DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

Após demonstrar a relação que a proteção aos dados pessoais possui com a preservação do direito à vida privada, um dos direitos da personalidade, é chegado o momento de traçar um panorama acerca das influências sofridas pelo Brasil para o surgimento da Lei Geral de Proteção de Dados Pessoais, a qual, conforme será visto, foi a primeira lei brasileira a disciplinar, expressamente e especificamente, a proteção aos dados pessoais.

Danilo Doneda (2020) aponta que a privacidade e a proteção de dados passaram a ter relevância jurídica, começando a ser debatidos doutrinariamente e enxergados como direitos fundamentais, em razão da evolução tecnológica, que teve como seu marco principal a Revolução Industrial. Prossequindo seu raciocínio, ele assevera que, após esse momento, a tecnologia, dotada de grande imprevisibilidade, impulsionou a eletrônica e as telecomunicações, e conseqüentemente, os rumos da sociedade, sendo que, através de seus mecanismos e instrumentos de controle, passou a oferecer riscos à privacidade.

Cientes da realidade que os cercava, Samuel D. Warren e Louis D. Brandeis (1890, p.196, apud Bastos; Pantoja; Dos Santos, 2021, on-line), publicaram o artigo “*The Right of Privacy*”, onde, buscando a consagração da privacidade como direito na Constituição norte-americana, aduziram que “a complexidade da vida em sociedade, e o avanço civilizacional que deu origem às tecnologias, também fez surgir a necessidade dos indivíduos terem um resguardo do exterior para os momentos em que estão sozinhos, o que se traduz como a privacidade.”

Naquele momento, de acordo com Lys Nunes Lugati e Juliana Evangelista de Almeida (2020), onde vigorava a primeira geração dos direitos fundamentais, a privacidade era baseada em ideias vinculadas à liberdade e ao individualismo e consistia em um direito negativo, ou seja, garantido se o Estado não se intrometesse na esfera individual dos cidadãos.

Patrícia Peck Pinheiro (2020) relata que, no contexto mundial, desde 1948, através da Declaração Universal dos Direitos Humanos, a privacidade é vista como um dos direitos humanos fundamentais, sendo que, com a expansão da era da sociedade digital, as instituições necessitaram resgatar e repactuar seus compromissos com os sujeitos sociais.

A previsão da privacidade como direito humano fundamental foi consagrada no artigo 12 da Declaração Universal dos Direitos Humanos:

Artigo 12 Ninguém será sujeito à interferência na sua vida privada, na sua família, no seu lar ou na sua correspondência, nem a ataque à sua honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques.

A visão individualista dos direitos fundamentais, segundo Lugati e Almeida (2020), começou a mudar nos anos 1960, com o desenvolvimento tecnológico e o crescimento da democratização da tutela da vida privada e de seu exercício, sendo que, em 1970, conforme aponta Mendes (2014, apud Lugati e Almeida, 2020, p. 4), surgiram “decisões jurídicas e legislações que afirmam que os dados pessoais são uma projeção da personalidade do indivíduo e por isso são hábeis a receber tutela jurídica.”

Nesse contexto, Rony Vainzof (2020) assevera que, no início dos anos 1970, o surgimento dos computadores fez crescer o uso do processamento de dados, inclusive os pessoais, sendo que, tal período coincide também com o surgimento dos blocos econômicos regionais, que acelerou a transmissão de dados pessoais em grande escala para o contexto mundial.

Sobre o contexto mundial naquele momento, Rony Vainzof (2020, p. 22) assevera ainda que “esse cenário revelou um aumento de produtividade e eficiência de empresas e governos e, por outro lado, também fez crescer a preocupação com a proteção da privacidade de indivíduos, sobretudo diante do fluxo transfronteiriço de dados.”

Diante da crescente preocupação com a proteção da privacidade individual, Danilo Doneda (2020, p. 164) relata que, “na década de 1970, surgiram as primeiras iniciativas legislativas para a tutela de dados pessoais”, sendo que tais leis compuseram a primeira geração de proteção aos dados pessoais, que durou até 1977, ano do surgimento da lei federal da República Federativa da Alemanha sobre proteção de dados pessoais

Sobre essa primeira geração, Doneda aponta o seguinte:

O núcleo destas leis era a concessão de autorizações para a criação destes bancos de dados e do seu controle a posteriori por órgãos públicos. Estas leis também enfatizavam o controle do uso de informações pessoais pelo Estado e pelas suas estruturas administrativas, que eram o destinatário principal (se não os únicos) destas normas. (DONEDA, 2020, p. 165)

Na medida em que essa geração começou a ficar obsoleta, Doneda (2020) menciona o surgimento da segunda geração de leis de proteção aos dados pessoais, a partir da segunda metade da década de 1970, a qual se caracterizava por apresentar uma nova estrutura, não baseada apenas no fenômeno computacional, mas também na avaliação de que a privacidade e a proteção dos dados pessoais consistiam em uma liberdade negativa, a ser exercida pelo cidadão, com base na Lei francesa de proteção aos dados pessoais, datada de 1978.

Cumprе trazer um importante destaque de Doneda sobre a nova geração:

Tal evolução refletia a insatisfação de cidadãos que sofriam com a utilização por terceiros de seus dados pessoais e careciam de instrumentos para defender diretamente seus interesses; além disso, o controle nos moldes das leis anteriores tornou-se inviável, dada a fragmentação dos polos de tratamento dos dados pessoais. Assim, criou-se um sistema que fornece instrumentos para o cidadão identificar o uso indevido de suas informações pessoais e propor a sua tutela. (DONEDA, 2020, p. 166)

Por sua vez, conforme Lugati e Almeida (2020), a terceira geração das referidas leis cuidava muito mais da garantia da efetividade do direito à privacidade do que da mera escolha de cessão ou não dos dados pessoais.

Nas palavras de Doneda (2020), essas leis, datadas da década de 1980, passaram a tratar a proteção de dados como algo muito mais complexo, que envolvia a participação do indivíduo na sociedade e considerava o contexto em que este deveria ceder seus dados, protegendo-o das ocasiões em que houvesse cerceamento circunstancial da sua liberdade decisória, a fim de garantir a efetividade do exercício da autodeterminação informativa, surgida como uma extensão das liberdades garantidas nas leis da geração anterior.

Inclusive, Doneda (2020) cita como um marco da consagração da autodeterminação informativa a sentença proferida pelo Tribunal Constitucional alemão em 1983, que se originou da desconfiança da população alemã acerca dos métodos de coleta de dados - principalmente em relação à lei que organizou o censo - e do destino que seria atribuído a estes nos trabalhos desenvolvidos pelo censo daquele ano, havendo desconfiança de que seriam utilizados para controle das atividades e da condição pessoal dos alemãos.

Segundo Doneda (2020), tal sentença, que até hoje é uma grande referência em se tratando de proteção a dados pessoais, reconheceu que as determinações da referida lei feriam a Constituição alemã no que se refere à tutela dos direitos da personalidade, declarando a inconstitucionalidade de parte de seus artigos, bem como a necessidade de ser observado o princípio da finalidade na coleta de dados, de modo que eventual diversidade de finalidades impediria o cidadão de conhecer o que efetivamente seria feito com suas informações e, ainda, mencionou o termo autodeterminação informativa pela primeira vez e foi precursora na valorização da proteção de dados pessoais como proteção à privacidade.

Lugati e Almeida (2020) criticam essa terceira geração, afirmando que só abarcou uma certa parcela de indivíduos, tornando-se insuficiente, o que deu azo ao surgimento da quarta geração de leis de proteção aos dados pessoais, válida até os tempos atuais.

A quarta geração das leis de proteção aos dados pessoais, segundo Doneda (2020), teve o fim de superar as dificuldades impostas pelo enfoque individual consagrado anteriormente, objetivando a criação de meios de proteção coletiva, voltados ao caso concreto, e reconhecendo a vulnerabilidade do titular dos dados frente às entidades coletoras de tais informações, que não poderia ser superada, meramente, pela autodeterminação informativa, vez que algumas formas de tratamento de dados precisam de proteção maior, a qual não poderia restringir-se à mera escolha individual.

Como visto, no Brasil, a preocupação com a proteção da privacidade e com a inviolabilidade dos dados pessoais como direitos fundamentais começou a aparecer a partir do advento da Constituição Federal, já dentro da quarta geração, conforme as já mencionadas disposições trazidas em seu artigo 5º, incisos X e XII.

Outro dispositivo legal que já demonstrava preocupação com a proteção aos dados pessoais em solo brasileiro é o Código de Defesa do Consumidor (Lei nº 8.078/1990), em seu artigo 43:

Art. 43. O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes.

§ 1º Os cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, não podendo conter informações negativas referentes a período superior a cinco anos.

§ 2º A abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele.

§ 3º O consumidor, sempre que encontrar inexatidão nos seus dados e cadastros, poderá exigir sua imediata correção, devendo o arquivista, no prazo de cinco dias úteis, comunicar a alteração aos eventuais destinatários das informações incorretas.

§ 4º Os bancos de dados e cadastros relativos a consumidores, os serviços de proteção ao crédito e congêneres são considerados entidades de caráter público.

§ 5º Consumada a prescrição relativa à cobrança de débitos do consumidor, não serão fornecidas, pelos respectivos Sistemas de Proteção ao Crédito, quaisquer informações que possam impedir ou dificultar novo acesso ao crédito junto aos fornecedores.

§ 6º Todas as informações de que trata o caput deste artigo devem ser disponibilizadas em formatos acessíveis, inclusive para a pessoa com deficiência, mediante solicitação do consumidor. (Incluído pela Lei nº 13.146, de 2015)

De acordo com Doneda (2020), o estabelecimento, pelo Código de Defesa do Consumidor, de direitos e garantias ao consumidor em relação aos seus dados cadastrados em bancos de dados teve o fim de equilibrar a relação de consumo através da imposição de limites ao uso destes pelo fornecedor, citando como exemplos disso o fato de que registros negativos sobre o consumidor não poderiam ser mantidos por mais que 5 anos, a necessidade de comunicação ao consumidor sobre o tratamento da informação em determinados casos, bem como o direito de acesso, correção e cancelamento justificado, e o fato de que a utilização dos dados pelo fornecedor deve limitar-se apenas aos fins pelos quais se deu a coleta.

Na Europa, Pinheiro (2020) aponta que a garantia do direito a proteção dos dados pessoais é vista como fundamental desde a sua previsão na Carta dos Direitos Fundamentais da União Europeia, datada de 07 de dezembro de 2000.

Além disso, conforme Pinheiro (2020), no ordenamento pátrio, havia a previsão quanto à proteção dos dados pessoais no Marco Civil da Internet, na Lei do Cadastro Positivo e no artigo 4º, inciso VII, do Decreto nº 7.962/2013, mas sem especificações quanto aos critérios para observar se existia o efetivo cumprimento dos padrões mínimos de segurança referentes à guarda, manuseio e descarte dos dados pessoais.

Pinheiro (2020) argumenta ainda que o Brasil e o resto do mundo somente passaram a pensar em desenvolver uma regulamentação específica protegendo os dados pessoais e prevendo punições ao descumprimento das regras a partir do momento em que a União Europeia promulgou o Regulamento Geral de Proteção de Dados Pessoais Europeu nº 679, em 27 de abril de 2016; destinado a proteger as pessoas físicas quanto ao tratamento dos dados pessoais e sua circulação. Segundo ela, essa preocupação mundial buscou, principalmente, evitar barreiras econômicas e manter relações comerciais e negociais com a União Europeia.

Destarte, sob a influência de todo o contexto de proteção de dados aqui relatado e do surgimento do Regulamento Geral de Proteção de Dados Pessoais Europeu, foi editada e promulgada em 14 de agosto de 2018, a Lei Geral de Proteção de Dados Pessoais no Brasil, cujos aspectos gerais serão explanados a seguir.

1.3 ASPECTOS GERAIS SOBRE A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

A Lei Geral de Proteção de Dados Pessoais (LGPD) foi promulgada em 14 de agosto de 2018, pelo ex-presidente da República Michel Temer, e conta com 65 artigos, divididos em 10 capítulos.

Antes de adentrar no tratamento de dados pessoais pelo Poder Público segundo a referida lei, é de grande relevância entender sua estrutura, esclarecendo aspectos sobre sua aplicabilidade, seus fundamentos, princípios orientadores e os requisitos para o tratamento de dados.

Como acontece em toda lei, o artigo 1º esteve destinado a apresentar o tema que a LGPD se destina a regulamentar, bem como os sujeitos sobre os quais se aplica e os direitos fundamentais que busca proteger:

Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Parágrafo único. As normas gerais contidas nesta Lei são de interesse nacional e devem ser observadas pela União, Estados, Distrito Federal e Municípios. (Incluído pela Lei nº 13.853, de 2019)

Conforme já relatado, a proteção aos dados pessoais tem o fim de resguardar, principalmente, o direito fundamental à vida privada, garantido na Constituição Federal. Além da privacidade, Pinheiro (2018, p. 37) defende que a LGPD buscou resguardar também os seguintes direitos fundamentais: “intimidade, honra, direito de imagem e dignidade.”

Sem limitar-se a comentar apenas o texto disposto no artigo 1º, Pinheiro (2018, p. 37) destaca que, através da globalização, cresceu a importância da obtenção de informações, as quais se tornaram “um ativo de alta relevância para governantes e empresários: quem tem acesso aos dados, tem acesso ao poder.”, o que deixa evidente que, além de proteger os dados pessoais, a promulgação da referida lei também objetivou resguardar os interesses das classes poderosas, para manutenção de suas relações comerciais e, conseqüentemente, de seu poder.

Ainda sobre o artigo 1º, Vainzof (2020) destaca que o mesmo se aplica tanto ao mundo virtual, quanto ao offline, para pessoas físicas ou jurídicas de direito público ou privado, e que o vocábulo “proteger” deixa claro que a lei leva em consideração a vulnerabilidade do titular dos dados em comparação aos agentes de tratamento destes.

Por sua vez, sobre o parágrafo único do artigo 1º da LGPD, Vainzof destaca o seguinte:

O parágrafo único em questão visa constringer a proliferação de regulamentações estaduais que certamente podem gerar potenciais controvérsias com a LGPD, mas não impede a capacidade legislativa dos entes federativos, o que seria resolvido apenas por meio de emenda constitucional, que inclusive já tramita no Congresso conforme PEC 17/2019, que além incluir a proteção de dados pessoais entre os direitos e garantias fundamentais, visa fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais (VAINZOF, 2020, p.24)

Na sequência, o artigo 2º da LGPD traz os principais fundamentos orientadores da disciplina da proteção de dados:

Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:

I - o respeito à privacidade;

II - a autodeterminação informativa;

III - a liberdade de expressão, de informação, de comunicação e de opinião;

IV - a inviolabilidade da intimidade, da honra e da imagem;

V - o desenvolvimento econômico e tecnológico e a inovação;

VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e

VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

De acordo com Vainzof (2020), a proteção à privacidade dada pelo inciso I tem a ver com sua consagração como direito fundamental nas principais constituições democráticas do mundo, e também com o fato de que é possível registrar em dados, ativa ou passivamente, tudo o que um indivíduo faz, motivo pelo qual a organização e compreensão dos dados torna a informação útil e capaz de ser armazenada e processada. Conclui seu raciocínio apontando que a privacidade surgiu como fundamento da LGPD para resguardar o direito do titular dos dados controlar a utilização destes por terceiros.

Sobre o inciso II, Vainzof (2020) assevera que a autodeterminação informativa surgiu como forma de garantir ao titular dos dados o controle e autoridade sobre o fluxo e o uso destes, conjugando, ao mesmo tempo, duas concepções de privacidade de dados, a saber, a negativa e estática, e a moderna, na qual a proteção é dinâmica e se manifesta durante todo o ciclo de vida dos dados, em todos os meios pelos quais circulem.

No contexto mundial, a consagração da autodeterminação informativa tem como marco a decisão

A disposição no inciso III que coloca como fundamento da LGPD a “liberdade de expressão, de informação, de comunicação e de opinião”, segundo Vainzof (2020), tem inspiração constitucional e de resguardo aos direitos humanos, considerando, por exemplo, ilícita a coleta de dados por órgãos públicos ou entidades privadas para utilizá-los a fim de criar dossiês contra jornalistas ou defensores dos direitos humanos, de forma a pressioná-los para que não exerçam a liberdade de expressão.

Ao mesmo tempo, Vainzof (2020) destaca que a garantia da liberdade de expressão, informação, comunicação e opinião deve ser equilibrada com a proteção à privacidade. Desse modo, o exercício de um desses direitos fundamentais não pode comprometer o outro, como acontece quando há o uso indevido dos dados pessoais, tema central do presente trabalho.

Podem ser destacados ainda como pertinentes a este estudo os incisos IV e VII, também inspirados na Constituição Federal (artigos 1º, III e 5º, X) e no Código Civil (artigos 20 e 21), conforme já adiantado nos tópicos anteriores.

Por sua vez, o artigo 3º, seus incisos e parágrafos, segundo Pinheiro (2018), dizem respeito à abrangência territorial do tratamento de dados, de maneira que a lei se aplica quando os dados forem coletados em território nacional, quando o objeto da operação (oferta de bens e serviços) ocorrer dentro do território nacional e quando o titular dos dados estiver em território nacional:

Art. 3º Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que:

I - a operação de tratamento seja realizada no território nacional;

II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou (Redação dada pela Lei nº 13.853, de 2019)

III - os dados pessoais objeto do tratamento tenham sido coletados no território nacional.

§ 1º Consideram-se coletados no território nacional os dados pessoais cujo titular nele se encontre no momento da coleta.

§ 2º Excetua-se do disposto no inciso I deste artigo o tratamento de dados previsto no inciso IV do caput do art. 4º desta Lei.

Na sequência, o artigo 4º da LGPD abrange as situações em que tal lei não é aplicável, demonstrando, segundo Pinheiro (2018, p. 41) “que o tratamento de dados pessoais deve seguir um propósito certo e funcional, mas que não supere a liberdade de informação e expressão, a soberania, segurança e a defesa do Estado.”

Ainda de acordo com Pinheiro (2018), como o foco da lei é regular atividades onde se oferecem bens ou serviços, não faria sentido serem abrangidas por ela atividades sem fins econômicos. Outra importante ressalva feita pela autora é que a delimitação do alcance da lei busca reduzir seus impactos econômicos e sociais, tendo em vista os altos custos envolvidos na implementação de todas as exigências trazidas pela norma.

O artigo 5º da LGPD traz alguns importantes conceitos sobre os termos utilizados na lei, que são os seguintes:

Art. 5º Para os fins desta Lei, considera-se:

I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável; II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural; III - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento; IV - banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico; V - titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento; VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais; VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador; VIII - encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD); (Redação dada pela Lei nº 13.853, de 2019) IX - agentes de tratamento: o controlador e o operador; X - tratamento: 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; XI - anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo; XII - consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada; XIII - bloqueio: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados; XIV - eliminação: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado; XV - transferência internacional de dados: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro; XVI - uso compartilhado de dados: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados; XVII - relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco; XVIII - órgão de pesquisa: 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; e (Redação dada pela Lei nº 13.853, de 2019) XIX - autoridade nacional: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional. (Redação dada pela Lei nº 13.853, de 2019)

Algumas das disposições constantes no artigo 5º da LGPD serão tratadas no segundo capítulo, destinado a estudar especificamente o tratamento de dados.

Mais à frente, o artigo 6º da LGPD coloca, junto à boa-fé, mais 10 princípios que deverão ser considerados no tratamento de dados:

Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:

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

II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

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

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

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

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

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

VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

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

Dentre esses 10 princípios, serão destacados quatro, a saber, o da finalidade, o da adequação, o da necessidade e o da transparência, eis que, segundo Vainzof (2020), constituem eles o cerne da LGPD, determinando, através do tratamento de dados, o respeito à proteção aos direitos fundamentais da liberdade, da privacidade e do livre desenvolvimento da personalidade da pessoa natural.

Com relação ao princípio da finalidade, Vainzof (2020) ensina que o mesmo possui grande importância prática, já que garante ao titular dos dados, por meio de prévia informação, as fronteiras quanto à legalidade do tratamento dos mesmos, demarcando o propósito do tratamento, desde que lícito, e dos terceiros que terão ou não acesso aos dados, objetivando a mitigação do risco de uso secundário à revelia do titular.

Em outras palavras, Doneda (2020, p. 170) resume o conceito, asseverando que para esse princípio, “toda utilização dos dados pessoais deve obedecer à finalidade conhecida pelo interessado antes da coleta de seus dados”.

Ademais, Vainzof (2020) explica que o princípio da finalidade tem tanta importância, que aparece expressamente em outros três princípios da LGPD, quais sejam, o da adequação, o da necessidade e o da qualidade dos dados.

Inclusive, apesar da relativa pouca idade da LGPD, já há tribunais se posicionando a favor da responsabilização civil de quem utiliza dados pessoais alheios de forma indevida e contrária ao que dispõe o princípio da finalidade:

APELAÇÃO CÍVEL. AÇÃO DECLARATÓRIA C/C OBRIGAÇÃO DE FAZER E REPARAÇÃO DE DANO MORAL. PRESTAÇÃO DE SERVIÇO DE INTERNET. SENTENÇA QUE JULGOU IMPROCEDENTES OS PEDIDOS COM FUNDAMENTO NO ART. 487 INCISO I DO CÓDIGO DE PROCESSO CIVIL. IRRESIGNAÇÃO DA PARTE AUTORA. CASO EM QUE PARA A CONTRATAÇÃO DE SERVIÇO DE INTERNET FOI CRIADO UM CNPJ EM NOME DA AUTORA COM POSTERIOR BAIXA. FALHA NO DEVER DE INFORMAÇÃO ADEQUADA E CLARA CONFIGURADA. DADOS PESSOAIS UTILIZADOS EM DETRIMENTO À FINALIDADE ESPECÍFICA, EXPLÍCITA E INFORMADA AO SEU TITULAR (ART. 6º, I, LGPD), POIS DESNECESSÁRIO A ABERTURA DE EMPRESA EM NOME DE PESSOA FÍSICA PARA A SIMPLES CONTRATAÇÃO DE SERVIÇOS DE INTERNET. DANO MORAL CONFIGURADO. NECESSIDADE DE REFORMA DA SENTENÇA. RECURSO CONHECIDO E PROVIDO. (TJ-PR - AC: 00766189320188160014 Paraná 0076618-93.2018.8.16.0014, Relator: Dartagnan Serpa Sa, Data de Julgamento: 10/05/2021, 7ª Câmara Cível) (grifo nosso)

No caso destacado, a empresa ré/apelada, para possibilitar a contratação de serviço de internet em nome da autora/apelante, criou um CNPJ em nome dela.

Ocorre que a autora/apelante era pessoa simples, e não tinha conhecimento de que a empresa seria aberta em nome dela, tendo sido induzida em erro, entendendo a ocorrência do fato apenas quando a empresa ré/apelada lhe fez uma ligação indagando sobre a existência de uma empresa em seu endereço, ocasião em que esclareceu que seu endereço era apenas residencial e possuía uma linha telefônica não solicitada.

Na ação, sustentou também que as conversas e áudios juntados aos autos não denotaram sua concordância com a abertura do CNPJ, tendo seguido apenas as orientações do vendedor da empresa ré/apelada para ter acesso aos serviços de internet, sendo que tal situação lhe ocasionou a violação de sua intimidade e privacidade, em virtude da exposição de seus dados pessoais a riscos, que justificam o pedido de indenização moral.

Após ter seu pedido julgado improcedente, a autora apelou e, como resultado, o TJ/PR entendeu ter a ré/apelada cometido falha no dever de informação adequada e clara, utilizando-se dos dados pessoais da autora/apelante em detrimento ao princípio da finalidade, disposto no artigo 6º, inciso I, LGPD, que impõe a quem faz o tratamento de dados pessoais o dever informar ao titular, de forma específica e explícita, sobre a finalidade da utilização de seus dados, sendo desnecessária a abertura de empresa em nome de pessoa física para realizar a contratação de serviços de internet.

Aparecendo no segundo inciso, o princípio da adequação também exerce grande importância na LGPD e, segundo Vainzof (2020), é uma vinculação com o princípio da finalidade, posto que o texto legal menciona que a adequação consiste na “compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento”.

Exemplificando a aplicação do princípio, Vainzof retrata a coleta de batimentos cardíacos diários de alguém por uma empresa especializada em feedbacks ao usuário sobre a manutenção de uma vida saudável:

Assim, se os batimentos cardíacos diários de alguém são coletados, por um relógio inteligente, e tratados, por uma empresa especializada em dar feedbacks ao usuário acerca da manutenção de uma vida saudável, desde que o titular seja informado previamente, com o consentimento específico e destacado (por serem dados sensíveis, nesse caso), o tratamento será considerado adequado. (VAINZOF, 2020, p. 132)

Mais um princípio de grande relevância, trazido no inciso III do artigo 6º da LGPD, é o da necessidade.

Nas palavras de Rafael Fernandes Maciel (2019, p. 23), o princípio da necessidade “impede que sejam tratados mais dados do que for necessário para atingir a finalidade informada. Os dados têm que ser pertinentes, proporcionais e não excessivos.”

No mesmo sentido, estabelece Vainzof:

A sua característica principal é a de ressaltar a limitação do tratamento ao mínimo necessário para se atingir a finalidade pretendida (Data Minimisation), mediante avaliação de quais espécies de dados são realmente imprescindíveis (dados pertinentes e não excessivos). (VAINZOF, 2020, p. 133)

Por fim, quanto ao princípio da transparência, disposto no inciso VI, Maciel (2019, p. 23) traz ao agente o dever de “prestar informações claras, precisas e facilmente acessíveis sobre a realização do tratamento, protegido os segredos comercial e industrial.”

Sobre a importância da transparência para garantia dos direitos fundamentais da privacidade e do livre desenvolvimento da personalidade, Vainzof assevera o seguinte:

Se o objetivo da legislação é tutelar direitos fundamentais, como privacidade e o livre desenvolvimento da personalidade, por meio do tratamento ético, responsável e seguro dos dados pessoais, não há como garantir referida tutela sem transparência, ou seja, sem que o titular dos dados tenha conhecimento de quem é o agente do tratamento e sobre as características do tratamento, com informações claras, precisas e facilmente acessíveis. (VAINZOF, 2020, p. 138)

Em continuação, o artigo 7º e seus incisos versam sobre as hipóteses de tratamento dos dados pessoais:

Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:

I - mediante o fornecimento de consentimento pelo titular;

II - para o cumprimento de obrigação legal ou regulatória pelo controlador;

III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;

IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;

V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;

VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;

VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro;

VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; (Redação dada pela Lei nº 13.853, de 2019)

IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou

X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

(...)

§ 3º O tratamento de dados pessoais cujo acesso é público deve considerar a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização.

§ 4º É dispensada a exigência do consentimento previsto no caput deste artigo para os dados tornados manifestamente públicos pelo titular, resguardados os direitos do titular e os princípios previstos nesta Lei.

§ 5º O controlador que obteve o consentimento referido no inciso I do caput deste artigo que necessitar comunicar ou compartilhar dados pessoais com outros controladores deverá obter consentimento específico do titular para esse fim, ressalvadas as hipóteses de dispensa do consentimento previstas nesta Lei.

§ 6º A eventual dispensa da exigência do consentimento não desobriga os agentes de tratamento das demais obrigações previstas nesta Lei, especialmente da observância dos princípios gerais e da garantia dos direitos do titular.

§ 7º O tratamento posterior dos dados pessoais a que se referem os §§ 3º e 4º deste artigo poderá ser realizado para novas finalidades, desde que observados os propósitos legítimos e específicos para o novo tratamento e a preservação dos direitos do titular, assim como os fundamentos e os princípios previstos nesta Lei.

Para o presente estudo, é relevante tecer comentários sobre os incisos I e III do artigo 7º da LGPD.

Como citado, o inciso I aponta que, para que haja tratamento de dados, deverá haver consentimento de seu titular.

Sabendo disso, Caio César Carvalho Lima (2020) conclui que as outras nove hipóteses têm sua validade independente do consentimento. Ademais, sobre o consentimento, o autor menciona que este deverá ser livre, informado e inequívoco, conforme dispõe o já citado artigo 5º, inciso XII, da LGPD.

Quanto ao termo “livre”, Lima (2020) explica que o consentimento deverá ser manifestado via escolha efetiva, e longe de qualquer pressão, pelo titular dos dados que serão tratados na operação.

Na sequência, com relação ao termo “informado”, Lima (2020) explica que este tem forte relação com o princípio da transparência, de forma que o titular dos dados deverá ser informado sobre o ciclo completo de vida do tratamento dos seus dados pessoais. Ele esclarece também que, como o artigo 8º da LGPD permite que o consentimento seja realizado por qualquer meio que manifeste a vontade do titular, essa transparência poderá, por consequência, ser levada a efeito das mais diversas formas.

Ainda, quanto ao termo “inequívoco”, Lima (2020) aponta que o controlador dos dados deverá demonstrar que o titular dos dados, de fato, manifestou a autorização de tratamento destes.

No que se refere ao inciso III do artigo 7º da LGPD, Lima (2020, p. 204) comenta que, o tratamento e o uso compartilhado de dados pelo Poder Público deverá objetivar, somente, a execução de políticas públicas (consistentes, segundo ele em “toda atividade realizada por qualquer ente da administração pública com o objetivo de solucionar demandas da sociedade, englobando setores, tais como saúde, educação, economia, entre outros”) expressamente previstas na legislação.

Os deveres e responsabilidades referentes ao tratamento de dados pelo Poder Público serão detalhados nos próximos capítulos.

Com relação ao artigo 9º, Pinheiro (2018) explica que este está ligado à transparência das informações do tratamento de dados, apontando como características ligadas ao livre acesso à informação a clara exposição, o fácil acesso relacionado à finalidade do tratamento, a forma, a duração e as informações relativas aos agentes que realizam o tratamento.

Já sobre o artigo 10 da LGPD, Pinheiro (2018), assevera que este se refere ao fato de que a finalidade apontada pelo controlador para o tratamento dos dados deve basear-se em fundamentação clara e legítima, devendo ser coletados apenas os dados realmente necessários, garantindo-se a proteção à privacidade de seu titular, e destaca também as obrigações da autoridade nacional de proteção de dados de proporcionar a emissão de relatórios acerca do tratamento e seus impactos e de respeitar as liberdades do controlador, como o segredo industrial e o comercial.

Portanto, considerando todos os princípios, fundamentos e requisitos constantes na LGPD, fica clara a complexidade envolvida no tratamento de dados, que será esmiuçado no capítulo seguinte.

2. TRATAMENTO DOS DADOS PESSOAIS

2.1 AGENTES DE TRATAMENTO DE DADOS E SUAS OBRIGAÇÕES

Como visto, em seus incisos, o artigo 5º da LGPD trouxe os principais conceitos referentes a proteção de dados pessoais, o que facilita, até mesmo aos leigos em Direito, a compreensão dos ditames dessa lei.

No inciso X deste artigo, é esclarecido que o tratamento de dados pessoais consiste em toda operação realizada com estes, sendo exemplificados os mais variados tipos de operações envolvendo informações pessoais.

E os responsáveis por tais operações são os agentes de tratamento de dados, os quais, segundo o inciso IX do mesmo artigo, são o controlador e o operador.

Segundo consta nos incisos VI e VII do artigo 5º da LGPD, o controlador e o operador são pessoas naturais ou jurídicas, de direito público ou privado, que possuem responsabilidades diferentes: enquanto o controlador toma as decisões referentes ao tratamento de dados pessoais, o operador realiza o tratamento de tais dados em nome do controlador.

Diante das disposições trazidas, é possível perceber que, enquanto o controlador exerce uma função de comando, o operador está mais ligado à efetiva execução da operação com dados pessoais.

Conhecidas as figuras do controlador e do operador, torna-se necessário trazer algumas das suas obrigações segundo a Lei Geral de Proteção de Dados Pessoais.

Nos termos do artigo 37 da LGPD, tanto o controlador, quanto o operador têm a obrigação de manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseadas no legítimo interesse.

Nas palavras de Pinheiro (2018), esse dever de documentação das operações serve de instrumento para manter o controle e a transparência das ações e garantir o cumprimento do propósito do tratamento de dados. Marcos Gomes da Silva Bruno (2020) complementa apontando que a manutenção do registro de operações auxilia ainda na mitigação dos riscos e no cumprimento do dever de prestação de contas trazido no artigo 6º, inciso X, da LGPD.

Maciel (2019) recomenda que a documentação do tratamento seja realizada sempre, inclusive para a ressalva de responsabilidades.

O artigo 38 da LGPD dispõe que se a autoridade nacional assim determinar, o controlador deverá elaborar relatório de impacto à proteção de dados pessoais, “inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial.”

Segundo Maciel (2019), essa obrigação está ligada às situações em que o tratamento de dados seja interesse legítimo da autoridade nacional de proteção de dados e onde sejam oferecidos riscos às liberdades civis e aos direitos fundamentais.

Esse relatório, segundo o parágrafo único do referido artigo, deverá conter, pelo menos, “a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados.”

Por sua vez, o artigo 39 da LGPD traz ao operador a obrigação de realizar o tratamento de dados de acordo com as orientações do controlador, que tem responsabilidade de verificar o cumprimento de suas instruções e das normas acerca da matéria tratada.

Pinheiro (2018) assevera que esse artigo traz expressamente a existência de vinculação entre controlador e operador, estabelecendo entre eles responsabilidade solidária a partir do momento em que ajustam suas vontades para realizar a operação, posto que, como o controlador é quem detém o consentimento do titular dos dados, permanece responsável pelo que ocorre no ciclo de vida dos dados pessoais na gestão e governança do negócio.

Ademais, os artigos 46 a 49 da LGPD trazem aos agentes de tratamento de dados pessoais a missão de buscar a manutenção da segurança e do sigilo dos dados, atribuindo-lhes os deveres de adotar todas as medidas e técnicas de segurança aptas a proteger os dados do acesso de pessoas não autorizadas, de formas de tratamento inadequado ou ilícito dos mesmos, bem como garantir a segurança da informação mesmo após o fim do tratamento dos dados, comunicar à autoridade nacional de proteção de dados qualquer incidente de segurança que ofereça risco aos titulares dos dados e garantir que a estruturação dos sistemas de tratamento de dados pessoais atendam aos requisitos de segurança, padrões de boas práticas e governança e os princípios gerais da LGPD.

Como se viu, a Lei Geral de Proteção de Dados Pessoais cuidou de elencar diversas responsabilidades ao controlador e ao operador, demonstrando grande preocupação em evitar que sejam ocasionados ao titular danos em razão do indevido manejo de seus dados.

Entretanto, se mesmo com toda essa regulamentação, ainda são cometidos erros, é possível imaginar a catástrofe que aconteceria se a lei fosse menos rígida, principalmente na atual era, onde o consumo de dados e informações cresce em progressão geométrica, dificultando ainda mais o controle, razão pela qual se demonstra acertada a opção do legislador em colocar mão mais firme sobre os agentes de tratamento de dados.

2.2 TIPOS DE DADOS SEGUNDO A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

Quando o assunto é tratamento de dados, além de conhecer os agentes responsáveis pelas operações com tais informações, é importante compreender também os tipos de dados retratados pela Lei Geral de Proteção de Dados Pessoais, eis que, a depender do tipo de dado que estiver recebendo tratamento, será diferente, também, a forma de protegê-lo.

O inciso I do artigo 5º da LGPD infere que dado pessoal é a “informação relacionada a pessoa natural identificada ou identificável”.

De acordo com Maciel (2019), os dados pessoais não se resumem aos nomes, prenomes, endereços e números de CPF, podendo ser considerados como tais todas as informações que identifiquem o indivíduo, mesmo que indiretamente, como por exemplo o número de identificação de funcionário em uma empresa ou até mesmo as características físicas de alguém. Ele explica também que existem dados que, enquanto sozinhos, não podem identificar a pessoa, mas quando associados a outros, devem ser considerados como dados pessoais.

Nas palavras de Vainzof (2020, p. 82), “é imprescindível, assim, seja diretamente, seja indiretamente, mesmo que em um segundo momento, ter o componente da identidade de uma pessoa natural como característica fundamental do dado pessoal.”

Ou seja, somente há que se falar em dado pessoal se este identificar uma pessoa natural. Nesse exato sentido, Maciel (2019, p. 25) assevera que “nomes de empresas, CNPJ e informações que não sejam relacionadas à pessoa natural não são dados pessoais.”

Noutro ponto, o inciso II do artigo 5º da LGPD dispõe que o dado pessoal sensível é aquele “sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.”

Nas palavras de Maciel (2019), dependendo da forma como esses dados forem utilizados, podem ser colocados em risco significativo alguns direitos e garantias fundamentais, sendo que, por tal razão, são submetidos a regime especial, sendo tratados de forma mais rigorosa, posto que, de acordo com Vainzof (2020), esse tipo de dado está mais suscetível a receber algum tipo de discriminação quando de seu tratamento.

Em razão da diferença de efeitos indesejáveis que o indevido tratamento de dados pessoais sensíveis pode causar, o artigo 11 da LGPD dispõe que só poderá haver operação sobre esses tipos de dados nas seguintes ocasiões:

Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:

I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;

II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:

- a) cumprimento de obrigação legal ou regulatória pelo controlador;
- b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;
- c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;
- d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem)
- e) proteção da vida ou da incolumidade física do titular ou de terceiro;
- f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou
- g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

Ou seja, em regra, o tratamento de dados sensíveis somente poderá ser realizado mediante consentimento específico e destacado, para finalidades específicas, ou sem o consentimento do titular, em situações excepcionais.

Inclusive, segundo Vainzof (2020), até mesmo o tratamento de dados em larga escala deverá ser realizado com cautela, posto que o cruzamento dos dados, principalmente se realizado de forma automatizada, pode resultar no processamento de dados sensíveis.

Por fim, o inciso III do artigo 5º da LGPD assevera que o dado anonimizado é aquele “relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento”.

Vainzof (2020) explica que a LGPD não considera esse tipo de dado como pessoal, razão pela qual não o protege, sendo que o mesmo acontece com os dados que anteriormente eram pessoais, mas passaram por “anonimização”, que consiste na utilização de técnicas através das quais os dados ficam impossibilitados de serem associados, direta ou indiretamente, a um indivíduo.

Nesse sentido, Maciel (2019) destaca, porém, que se o titular puder, deverá optar por não realizar a anonimização de seus dados pessoais, posto que esse é um processo arriscado, justamente pela falta de proteção legal sobre o dado que passar por esse tipo de processo. Além disso, ele relata também que um dado pode deixar de ser anônimo se o processo de anonimização ao qual foi submetido for revertido.

Outro aspecto que deve ser elucidado neste ponto, é o disposto no artigo 13 da LGPD:

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

De acordo com Maciel (2019), a pseudonimização é um processo que também pode ser considerado para diminuir os riscos de manejo indevido de dados pessoais e validar o cumprimento dos princípios da necessidade e adequação na concepção de um produto ou serviço, sendo que, ele aponta também serem bastante pertinentes ao processo de pseudonimização outras características, tais quais a descentralização, a transparência, o consenso e a segurança.

As distinções sobre dados aqui trazidas fazem parte de um ponto positivo a ser destacado acerca da LGPD, já que, ao estabelecer essas diferenciações, o legislador permitiu que se entendesse o porquê de alguns dados merecerem maior proteção e outros uma proteção menos robusta, já que, quanto mais íntimo for determinado dado, mais atrelado ele estará aos direitos da personalidade do seu titular, e, por consequência, necessitará de proteção mais abrangente.

2.3 TÉRMINO DO TRATAMENTO DE DADOS

Nas palavras de Pinheiro (2018), o tratamento de dados tem alguns limites, que podem estar relacionados tanto às informações coletadas, quanto ao tempo de duração do procedimento, o qual, portanto, não pode dar-se por período indeterminado.

Nesse sentido, a LGPD reservou a seção IV do seu capítulo II para tratar, nos artigos 15 e 16, sobre o término do tratamento de dados.

O artigo 15 elenca, em seus incisos, as quatro principais hipóteses de término do tratamento de dados:

Art. 15. O término do tratamento de dados pessoais ocorrerá nas seguintes hipóteses:
I - verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada;
II - fim do período de tratamento;
III - comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento conforme disposto no § 5º do art. 8º desta Lei, resguardado o interesse público; ou
IV - determinação da autoridade nacional, quando houver violação ao disposto nesta Lei.

Tais hipóteses, contudo, não são taxativas, asseverando Maciel (2019), que o término do tratamento de dados poderá ser interrompido por opção do controlador ou através da revogação da lei ou regulamento que lhe dava base legal.

Segundo Lima (2020), o inciso I desse artigo reforça a importância dada pelo legislador ao princípio da finalidade, ao dispor que quando a finalidade for alcançada ou os dados deixarem de ser necessários ao seu alcance, deverá haver o encerramento do tratamento.

Quanto ao inciso II, Lima (2020) esclarece que este diz respeito ao tratamento de dados que possui prazo determinado, de forma que, findo esse, os dados não poderão mais ser tratados.

Em seguida, Lima (2020) aponta que o inciso III está ligado à ocorrência de expressa solicitação de exclusão dos dados pelo titular, que encerra o tratamento de dados, exceto nas hipóteses de manutenção de dados previstas em lei. O autor entende, porém, que se essa mera revogação do consentimento não for seguida de pedido expresso de exclusão dos dados, estará autorizada a manutenção dos dados, ratificando-se os tratamentos até aquele momento realizados.

Por fim, no que se refere ao inciso IV, Lima (2020) aponta que a Autoridade Nacional de Proteção de Dados poderá ordenar a certo agente de tratamento de dados a obrigação de eliminar os dados quando encontrar dificuldade em comprovar sua licitude.

Na sequência, o artigo 16 da LGPD trata sobre a regra geral de que os dados pessoais deverão ser eliminados após seu uso e traz as exceções nas quais é autorizada sua conservação:

Art. 16. Os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades:

I - cumprimento de obrigação legal ou regulatória pelo controlador;

II - estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;

III - transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou

IV - uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.

Sobre tal dispositivo legal, Pinheiro (2018) esclarece que as instituições buscam, sempre que possível, evitar a eliminação dos dados pessoais, objetivando preservar a base destes, pois há altos valores envolvidos na manutenção da informação, salientando que, apesar de o descarte ser um direito, antes dele ser realizado, deverá ser observado se existe alguma justificativa legal plausível para que os dados sejam mantidos até sua eliminação em definitivo.

Pinheiro (2018) complementa que o debate sobre as possibilidades de apagamento ou retenção dos dados reside no confronto entre o direito ao esquecimento e o direito à portabilidade dos dados, que trazem grande impacto à gestão do ciclo de vida destes,

destacando, por fim, que uma alternativa que tem se mostrado viável à continuidade do armazenamento da informação é a anonimização dos dados.

Com relação ao inciso I, Lima (2020) dispara que este está ligado ao cumprimento, pelo controlador, de obrigações legais cuja observância é mais importante do que o dever de eliminação dos dados. Ele assevera, ainda que tal dispositivo poderá ser aplicado também ao operador que se encontrar em situação semelhante.

Sobre o inciso II, Lima (2020) explica que, quando o armazenamento dos dados estiver a cargo dos órgãos de pesquisa, estes poderão mantê-los em sua base por prazo indeterminado, sendo recomendado, contudo, que anonimizem tais dados.

Já o inciso III, segundo Lima (2020), refere-se à situação específica em que haja motivação para que os dados sejam retidos a fim de que, futuramente, sejam transferidos a terceiros, devendo todos os dispositivos da LGPD serem respeitados para que isso se concretize.

Por último, ao comentar a possibilidade de manutenção dos dados para uso exclusivo do controlador, desde que estejam anonimizados, Pinheiro (2018) critica a redação do inciso IV, asseverando que não faz sentido a proibição do acesso de terceiros aos dados anonimizados, posto que estes não são regulados pela LGPD.

2.4 OS DIREITOS DO TITULAR DE DADOS

Após tratar acerca do encerramento do tratamento de dados, a LGPD cuidou, no capítulo III de sua seção IV, dos direitos do titular dos dados.

O já citado artigo 5º, inciso V da LGPD menciona que o titular é a “pessoa natural a quem se referem os dados pessoais que são objeto de tratamento”.

Portanto, como argumenta Maciel (2019), os dados de pessoas jurídicas não são disciplinados da LGPD. Entretanto, para evitar que sejam criadas confusões, o autor ressalva que os dados das pessoas naturais que exerçam a função de representante legal das pessoas jurídicas se sujeitam às regras de tratamento de dados, de modo que tais sujeitos terão direitos como titulares dos dados.

Segundo consta no artigo 17 da LGPD, “toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade (...)”.

Sobre tal dispositivo legal, Pinheiro (2018) comenta que um dos principais objetivos da LGPD é garantir a proteção e o livre desenvolvimento da pessoa natural, sendo que a garantia de titularidade dos dados pessoais à pessoa natural está intimamente ligada à inviolabilidade da

vida privada, trazida no artigo 5º, inciso X da Constituição Federal e no artigo 21 do Código Civil, conforme retratado, também, no primeiro capítulo deste trabalho.

Em continuidade, o artigo 18 da LGPD traz, em seus incisos, tudo o que pode ser solicitado, a qualquer momento e, mediante requisição, pelo titular dos dados ao controlador destes:

Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:

I - confirmação da existência de tratamento;

II - acesso aos dados;

III - correção de dados incompletos, inexatos ou desatualizados;

IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;

V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial; (Redação dada pela Lei nº 13.853, de 2019)

VI - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei;

VII - informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;

VIII - informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;

IX - revogação do consentimento, nos termos do § 5º do art. 8º desta Lei.

§ 1º O titular dos dados pessoais tem o direito de peticionar em relação aos seus dados contra o controlador perante a autoridade nacional.

§ 2º O titular pode opor-se a tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, em caso de descumprimento ao disposto nesta Lei.

§ 3º Os direitos previstos neste artigo serão exercidos mediante requerimento expresso do titular ou de representante legalmente constituído, a agente de tratamento.

§ 4º Em caso de impossibilidade de adoção imediata da providência de que trata o § 3º deste artigo, o controlador enviará ao titular resposta em que poderá:

I - comunicar que não é agente de tratamento dos dados e indicar, sempre que possível, o agente; ou

II - indicar as razões de fato ou de direito que impedem a adoção imediata da providência.

§ 5º O requerimento referido no § 3º deste artigo será atendido sem custos para o titular, nos prazos e nos termos previstos em regulamento.

§ 6º O responsável deverá informar, de maneira imediata, aos agentes de tratamento com os quais tenha realizado uso compartilhado de dados a correção, a eliminação, a anonimização ou o bloqueio dos dados, para que repitam idêntico procedimento, exceto nos casos em que esta comunicação seja comprovadamente impossível ou implique esforço desproporcional. (Redação dada pela Lei nº 13.853, de 2019)

§ 7º A portabilidade dos dados pessoais a que se refere o inciso V do caput deste artigo não inclui dados que já tenham sido anonimizados pelo controlador.

§ 8º O direito a que se refere o § 1º deste artigo também poderá ser exercido perante os organismos de defesa do consumidor.

A preocupação do artigo 18, segundo Pinheiro (2018), é garantir que o titular tenha o direito de verificar se seus dados estão sendo tratados de forma segura, verídica e com o cumprimento da finalidade.

Maldonado (2020) comenta que nem sempre é possível o atendimento de todas as requisições do titular dos dados, de modo que o próprio §4º do artigo 18 da LGPD retrata hipóteses em que é impossível o atendimento da pretensão. Contudo, ele assevera que a ideia da lei, é no sentido de que, ainda que seja impossível esse atendimento, o controlador tem o dever de analisar toda requisição que lhe for formulada, não podendo ignorá-la, mesmo que seja ilegítima ou despropositada.

Como comenta Maldonado (2020), o inciso I do artigo 18, o qual versa sobre a possibilidade de o titular verificar se o tratamento de seus dados pessoais realmente existe, tem a ver com o princípio da transparência e busca garantir ao titular dos dados o controle permanente de tais informações, mesmo que estas tenham sido disponibilizadas no momento do recolhimento dos dados.

No que concerne ao inciso II, referente ao direito de acesso aos dados, Maldonado (2020) expõe que tal direito valida a presunção de conhecimento prévio ou de anterior confirmação da existência do tratamento pelo titular, de modo que este, uma vez incontroversa a existência do tratamento, poderá ter acesso a um amplo rol de informações, tais quais, para exemplificar, a origem dos dados, a finalidade de seu uso, as categorias, os destinatários, a existência de decisões automatizadas e o prazo de conservação.

Por sua vez, quanto ao inciso III, Maldonado (2020) esclarece que a preocupação da LGPD com a correção de dados incompletos, inexatos ou desatualizados tem a ver com a necessidade de identificação de pessoas dentro do território nacional, vez que a falta de acurácia nos dados pode facilitar fraudes, principalmente virtuais, razão pela qual qualquer mudança nas informações do titular enseja a necessidade de atualização dos dados, que deve dar-se mediante provocação do interessado.

Quanto ao inciso IV, que diz respeito a anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a LGPD, Maciel (2019) aponta que, apesar de o controlador possuir o direito de definir qual o melhor processo técnico a ser utilizado em cada situação, deverá cessar o tratamento quando houver esses excessos ou descumprimento da LGPD.

Maciel (2019) aduz também, que o inciso V, ao versar sobre o direito à portabilidade, busca a proteção dos segredos comercial e industrial. A obra citada foi anterior à promulgação da Lei nº 13.853/2019, a qual retirou a parte do dispositivo que determinava a necessidade da regulamentação da portabilidade pelo órgão controlador, mas a autora, em consonância com a lei que estava por vir, já criticava essa necessidade, principalmente em se tratando de serviços digitais, posto que os sistemas de proteção de dados de cada empresa foram criados mais para

evitar o uso pelos concorrentes do que para integrar o uso comum, defendendo assim que a validade desse direito não dependeria de regulamento futuro pela Autoridade Nacional de Proteção de Dados.

Com relação ao inciso VI, Maldonado (2020) explica que, assim como o titular poderá conceder o uso de seus dados, tem o direito também de retirar tal consentimento quando quiser. Sendo assim, nada mais justo que, deixando de existir o consentimento, o titular possa postular a eliminação de seus dados, salvo se presente alguma das exceções do artigo 16 da LGPD, ocasião em que a negativa deverá ser imediatamente comunicada e justificada ao titular dos dados.

O inciso VII tem a ver com o uso compartilhado de dados com entidades públicas e privadas pelo controlador.

Sobre tal inciso, importante trazer a seguinte interpretação de Maciel:

O artigo 9º prevê o dever de informar ao titular sobre situações de tratamento de dados, dentre as quais está se o controlador faz uso compartilhado de dados explicitando também a finalidade desse compartilhamento. O artigo 18, por sua vez, trata do dever de informar mediante requerimento do titular. Assim, da leitura conjunta de ambos, temos que sem solicitação, o controlador deve apenas informar se há compartilhamento de dados e sua respectiva finalidade. Mediante requerimento expresso do titular, sob espeque do artigo 18, deve o controlador nominar expressamente as entidades públicas e privadas que acessam os dados de forma compartilhada. (MACIEL, 2019, p. 44)

Complementando a interpretação supra, Viviane Nóbrega Maldonado (2020) aponta que a intenção desse dispositivo legal é garantir ao titular o pleno controle de seus dados pessoais, tendo ciência acerca de todas as entidades, públicas ou privadas que tratem tais informações, através do mencionado compartilhamento pelo controlador.

O inciso VIII, de acordo com Maciel (2019), diz respeito ao direito de o titular ser informado sobre as consequências que pode sofrer em virtude de eventual não consentimento quando o tratamento de dados exige-lo. Ele ressalva, contudo, que como o tratamento de dados deve respeitar a finalidade, a necessidade e a adequação, este não poderá ser realizado se o titular não consentir com o manejo de certo dado pessoal que não seria necessário para atingir sua finalidade.

Ainda tratando o inciso, Maciel (2019) assevera que, se a falta de consentimento ocasionar limitações parciais ao uso, o titular dos dados deverá ser informado e alertado e que a limitação total só poderá ocorrer se o uso do dado for extremamente necessário e adequado para atingir a finalidade.

O último inciso do artigo 18, de número IX, diz respeito ao direito de revogação do consentimento pelo titular, que segundo Pinheiro (2018), é um reflexo de sua liberdade de escolha, e, assim como o consentimento, deverá ser expresso.

Com relação às formas de atendimento às solicitações dos titulares, destacadas nos parágrafos do artigo 18 e no artigo 19 da LGPD, Maciel (2019) aponta, em primeiro lugar, que estas deverão ser endereçadas somente ao controlador, que deverá atendê-las em sua amplitude, já que o operador não tem o dever legal de atender às indagações do titular de dados.

Das disposições acerca do atendimento às solicitações, Maciel (2019) faz vários destaques. Em primeiro lugar, o autor aponta que o requerimento de informações deverá ser expresso, conforme artigo 18, §3º da LGPD, sendo que, em contrapartida, conforme o §4º, se o controlador não puder atendê-lo de forma imediata, deverá justificar as razões que impeçam a adoção imediata de providências ou que não é o agente de tratamento responsável, indicando aquele que seja.

Ademais, Maciel (2019) tece críticas às disposições dos §§7º e 8º do artigo 18 da LGPD, afirmando que não seria necessária disposição legal acerca da não aplicabilidade do direito de portabilidade a dados anonimizados, vez que a lei já foi clara ao dispor que não disciplina esse tipo de dados, e não seria necessário, também, dispor sobre a possibilidade de o exercício do direito de petição à ANPD em face do controlador (artigo 18, §1º, LGPD), nos organismos de defesa do consumidor.

Na sequência, o artigo 19 da LGPD traz os seguintes termos:

Art. 19. A confirmação de existência ou o acesso a dados pessoais serão providenciados, mediante requisição do titular:

I - em formato simplificado, imediatamente; ou

II - por meio de declaração clara e completa, que indique a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento, observados os segredos comercial e industrial, fornecida no prazo de até 15 (quinze) dias, contado da data do requerimento do titular.

§ 1º Os dados pessoais serão armazenados em formato que favoreça o exercício do direito de acesso.

§ 2º As informações e os dados poderão ser fornecidos, a critério do titular:

I - por meio eletrônico, seguro e idôneo para esse fim; ou

II - sob forma impressa.

§ 3º Quando o tratamento tiver origem no consentimento do titular ou em contrato, o titular poderá solicitar cópia eletrônica integral de seus dados pessoais, observados os segredos comercial e industrial, nos termos de regulamentação da autoridade nacional, em formato que permita a sua utilização subsequente, inclusive em outras operações de tratamento.

§ 4º A autoridade nacional poderá dispor de forma diferenciada acerca dos prazos previstos nos incisos I e II do caput deste artigo para os setores específicos.

Tal dispositivo, como se vê, tem caráter nitidamente procedimental, indicando como deverá ser a requisição do titular para confirmar a existência ou acesso a seus dados pessoais, bem como os meios de armazenamento e o fornecimento dos dados.

Outro importante direito do titular de dados pessoais está disposto no artigo 20 da LGPD, segundo o qual esse sujeito poderá solicitar a revisão das decisões tomadas com base em tratamento automatizado dos dados, desde que isso afete seus interesses, inclusive “as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.” Eis os termos do artigo 20 da LGPD:

Art. 20. O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade. (Redação dada pela Lei nº 13.853, de 2019) Vigência

§ 1º O controlador deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial.

§ 2º Em caso de não oferecimento de informações de que trata o § 1º deste artigo baseado na observância de segredo comercial e industrial, a autoridade nacional poderá realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais.

De acordo com Laura Secfém Rodrigues e Márcio Pompeu (2021, on-line), “esse direito é necessário, na medida em que o uso da inteligência artificial também está sujeito a erros, por deficiência tecnológica ou até pelo uso de uma base de dados limitada ou incompleta.”. Os autores salientam, também, que já é possível verificar vários equívocos em decisões algorítmicas, gerando danos aos titulares de dados, de modo que a previsão do artigo 20 da LGPD é bastante acertada, diante do crescente uso de tecnologias na sociedade atual.

Na sequência, o artigo 21 da LGPD determina que “os dados pessoais referentes ao exercício regular de direitos pelo titular não podem ser utilizados em seu prejuízo.”

A proteção oferecida por esse dispositivo legal é plenamente compreensível, eis que, conforme ressalta Pinheiro (2018, p. 62), “o consentimento do titular ao tratamento de seus dados pessoais não deve lhe onerar de forma alguma”.

Essa parte da LGPD pode ser confrontada com a Resolução STF nº 759, de 17 de dezembro de 2021, a qual, segundo consta em sua ementa, “instituiu a Política de Privacidade e de Proteção de Dados Pessoais no âmbito do Supremo Tribunal Federal” (BRASIL, 2021, on-line), dispondo o seguinte em seu artigo 5º:

Art. 5º O STF poderá, nas atividades voltadas ao estrito exercício de suas competências e de acordo com os princípios e as bases legais estipuladas pela LGPD, proceder ao tratamento de dados pessoais **independentemente de consentimento dos titulares. (grifo nosso)**

Parágrafo único. No exercício de atividades administrativas não vinculadas diretamente ao exercício de suas competências legais e constitucionais, o STF deverá obter o consentimento dos titulares para tratar seus dados pessoais, sempre respeitando e concretizando a autodeterminação informativa dos envolvidos.

Se a interpretação dessa Resolução se baseasse somente nas disposições da parte final do caput do seu artigo 5º, certamente, pareceria que foram dados amplos poderes ao Supremo Tribunal Federal como agente de tratamento de dados, enfraquecendo um dos principais requisitos à tal operação: o consentimento do titular.

Porém, a leitura do parágrafo único do mesmo artigo já permite perceber que o tratamento de dados independentemente de consentimento é hipótese de exceção, cabível apenas no que se refere ao exercício das competências específicas do STF, e limitado pelas disposições da LGPD, sendo que, quanto às funções administrativas do Supremo, o consentimento do titular dos dados ao tratamento ainda é imprescindível.

Ademais, o tratamento dos dados pessoais pelo STF nas hipóteses trazidas deverá diversos procedimentos e regras, trazidos principalmente entre os artigos 6º a 12 da LGPD:

Art. 6º Os dados pessoais tratados pelo STF serão:

I - protegidos por procedimentos internos, com trilhas de auditoria para registrar autorizações, utilização, impactos e violações;

II - mantidos disponíveis, exatos, adequados, pertinentes e atualizados, sendo retificados ou eliminados mediante informação ou constatação de impropriedade ou face a solicitação de remoção, devendo a neutralização ou descarte do dado observar as condições e períodos da tabela de prazos de retenção de dados;

III - compartilhados somente para o exercício das atividades voltadas ao estrito exercício de suas competências legais e constitucionais, ou para atendimento de políticas públicas aplicáveis; e

IV - revistos em periodicidade mínima anual, sendo de imediato eliminados aqueles que já não forem necessários, por terem cumprido sua finalidade ou por ter encerrado o seu prazo de retenção.

Art. 7º A responsabilidade do STF pelo tratamento de dados pessoais estará circunscrita aos deveres decorrentes do exercício de suas atribuições constitucionais, legais e institucionais, pautando-se pelo princípio da prestação de contas, com emprego e demonstração das boas práticas de governança e de segurança da informação a fim de cumprir as normas de proteção de dados pessoais por meio de medidas eficazes.

Art. 8º O STF deverá adotar todas as medidas possíveis para garantir o usufruto dos direitos assegurados pela LGPD ao titular dos dados pessoais, bem como pelas legislações e atos normativos correlatos, informando adequadamente os procedimentos necessários à sua fruição nos respectivos sítios eletrônicos e materiais de divulgação específicos.

Art. 9º Os contratos firmados pelo STF com terceiros serão, gradativamente, adaptados para, no que couber, alinharem-se a esta Política. Parágrafo único. Os contratos em vigor poderão ser revistos para adaptação e adequação a esta Política, e, dentro de suas particularidades, serem aditados ou regidos por disciplina própria para a consecução dessa reformulação.

Art. 10. Os dados pessoais sensíveis tratados na atividade jurisdicional independem de consentimento, com base no art. 11, II, a e b, da LGPD, sem prejuízo da observância de outras prescrições de tratamento de dados previstas na legislação processual. Parágrafo único. Em relação às ações administrativas, o tratamento de dados sensíveis deverá se fundamentar nas hipóteses do art. 11, II, da LGPD, comprovando-se a indispensabilidade do tratamento e publicidade nos casos de eventual dispensa de consentimento, na forma do art. 23, I, da LGPD e de eventual

disposição da Autoridade Nacional de Proteção de Dados (ANPD), em regulamento ou ato específico para regência de cada relação jurídica.

Art. 11. O tratamento de dados de criança e adolescente deve se pautar pelo seu melhor interesse e por sua máxima proteção, devendo o STF disponibilizar as informações sobre o tratamento realizado de maneira simples, clara e acessível, proporcionando o seu pleno entendimento por parte da criança, do adolescente, dos pais e dos responsáveis legais. § 1º Para fins desta Política, considera-se criança os menores de 16 anos e adolescente aqueles entre 16 e 18 anos. § 2º O tratamento de dados de adolescente seguirá adicionalmente as regras civis e penais aplicáveis. § 3º É vedado o repasse de dados pessoais de criança a terceiro sem o consentimento específico e destacado de um de seus pais ou responsáveis legais, neste último caso com a obrigação de o STF realizar esforços razoáveis e tecnologicamente possíveis para verificação da higidez do consentimento fornecido e da veracidade do responsável, mantendo pública a informação acerca dos dados coletados, da forma de sua utilização e dos procedimentos para o pleno exercício dos direitos do titular dos dados, nos termos do art. 14, §2º c/c art. 18 da LGPD. §4º O tratamento de dados de criança na atividade jurisdicional e administrativa do Tribunal admite excepcionalmente a dispensa fundamentada do consentimento elencado no art. 14, §1º, da LGPD, quando tal medida for estritamente necessária para sua proteção e seu melhor interesse, assim como quando a coleta for necessária para contatar os pais ou responsáveis legais, de acordo com o art. 14, §3º, da LGPD.

Art. 12. Os portais do STF na internet poderão utilizar arquivos (cookies) para registrar e gravar, no computador do usuário, as preferências e navegações realizadas nas respectivas páginas, para fins estatísticos e de aprimoramento dos serviços, desde que obtido o consentimento do titular e respeitadas as normas de proteção de dados pessoais.

Por fim, o artigo 22 da LGPD traz ao titular dos dados pessoais a possibilidade de defesa de seus interesses e direitos em juízo, individual ou coletivamente.

Maldonado (2020) assevera que o exercício desses direitos em juízo não impede a instauração de procedimentos administrativos perante à Agência Nacional de Proteção de Dados (artigo 55-J, inciso IV, LGPD). Além disso, a autora salienta que o objetivo do legislador ao trazer esse dispositivo foi o de possibilitar a ampla proteção ao titular de dados, que é a figura central da LGPD, disponibilizando a tal sujeito inúmeras garantias para defesa de seus direitos.

Diante de tudo que foi trazido, é possível perceber que a pessoa física, grande protegida pela LGPD, possui inúmeros direitos a serem exercidos para fiscalizar o tratamento dos seus dados pessoais, devendo, para tanto, buscar a provocação do controlador de dados para que seus requerimentos em relação ao tratamento sejam atendidos, de modo que, como o titular dos dados é a prioridade da comentada lei, mesmo que não seja possível o atendimento das solicitações, o controlador deverá, obrigatoriamente, analisar todas as provocações que lhe forem feitas, apresentando sempre respostas justificadas a estas, principalmente se forem negativas.

3. ATIVIDADE ESTATAL E O SISTEMA DE PROTEÇÃO DE DADOS

3.1 TRATAMENTO DOS DADOS PESSOAIS PELO PODER PÚBLICO

Conforme ensina Tasso (2020), a assimetria de poder é a principal marca da relação entre o Poder Público e o titular de dados pessoais, em vista tanto do poder de império exercido pelo primeiro, quanto pela circunstância objetiva de o ente estatal possuir uma grande quantidade de dados pessoais em sua base, em razão da atividade que desempenha. O autor comenta também que, no tratamento de dados pelo Estado, há a gestão de muitos dados potencialmente sensíveis, de modo que a massificação e voracidade da coleta de dados, tratados de forma não padronizada, pode implicar na violação de direitos e garantias de seu titular

Diante dessa relação desequilibrada, surgiu a necessidade de proteção do titular dos dados tratados pelo Poder Público, levando em consideração principalmente a existência dos riscos de violações a seus direitos.

Como exemplos dessa proteção, podem ser citadas as decisões proferidas pelo Supremo Tribunal Federal nas Ações Diretas de Inconstitucionalidade de nº 6387, 6388, 6389, 6390 e 6393, conforme consta no portal de notícias do STF (2020).

Tais ações, que passaram a tramitar juntas, conforme decisão do Supremo (STF, 2020), foram propostas contra o inteiro teor da Medida Provisória nº 954, de 17 de abril de 2020, a qual tinha a seguinte ementa:

Dispõe sobre o compartilhamento de dados por empresas de telecomunicações prestadoras de Serviço Telefônico Fixo Comutado e de Serviço Móvel Pessoal com a Fundação Instituto Brasileiro de Geografia e Estatística, para fins de suporte à produção estatística oficial durante a situação de emergência de saúde pública de importância internacional decorrente do coronavírus (covid-19), de que trata a Lei nº 13.979, de 6 de fevereiro de 2020. (BRASIL, 2020)

Nas ADI nº 6.387, movida pelo Conselho Federal da OAB e que serviu de base da aplicabilidade da decisão às outras 4 ADI's, segundo consta na decisão (STF,2020), asseverou-se que a referida Medida Provisória continha vícios formais, referentes a não observância dos requisitos constitucionais para a edição desse tipo legislativo, que são a urgência e a relevância material autorizadora (art. 62, CF), vez que não foi justificada a importância da solicitação de compartilhamento de dados, nem demonstrada a contribuição que a medida daria para a formulação de políticas públicas de combate à crise sanitária decorrente da pandemia da covid-19, diante da ausência de informação de quais tipos de pesquisas seriam realizadas.

Ainda conforme a decisão (STF, 2020) foram suscitados vícios materiais em razão do descumprimento dos princípios constitucionais da dignidade da pessoa humana (art. 1º, III, CF),

da inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas (art. 5º, X, CF), do sigilo dos dados (art. 5º, XII, CF) e da autodeterminação informativa, conforme a LGPD.

Inclusive, o Conselho Federal da OAB, autor da ação, invocou como um de seus argumentos a decisão proferida pelo Tribunal Constitucional alemão em 1983 – e tratada no 1º capítulo -, a qual reconheceu, com base no direito geral da personalidade, o direito à autodeterminação informativa em face de intervenções estatais e a não observância da proporcionalidade, eis que não foi esclarecida a finalidade específica de uso da pesquisa estatística, nem a adequação e necessidade dos dados, tampouco a proteção que seria dada aos titulares nesse tratamento de dados (STF, 2020).

Dessa forma, conforme relatório da decisão (STF, 2020), foi requerida pelo órgão da classe advocatícia medida cautelar, com base no art. 10, §3º da Lei nº 9.868/1999 para suspender, com base na plausibilidade do direito (em razão da falta dos requisitos constitucionais autorizadores e da violação aos princípios constitucionais mencionados) e a urgência (por conta do curto prazo de três dias para divulgação do procedimento para disponibilização dos dados – art. 2º, §2º, MP nº 954/2020) a eficácia do inteiro teor da MP até o julgamento da ação, onde pleiteou fosse declarada inconstitucional o referido tipo legislativo.

Adentrando ao mérito da decisão (STF, 2020), a Ministra Rosa Weber, relatora da ação, consignou que os dados sobre os quais o art. 2º da MP impôs a obrigação de divulgação às empresas prestadoras de serviços telefônicos fixos e móveis, a saber, nomes, números de telefone e endereço dos consumidores são pessoais, devendo seu tratamento observar a proteção constitucional ao livre desenvolvimento da personalidade, à privacidade e à liberdade individual, bem como aos fundamentos específicos da proteção aos dados individuais dispostos no art. 2º, I e III da LGPD, a saber, a própria privacidade e a autodeterminação informativa.

Em seguida, a relatora consignou que o art. 2º, §1º da MP, destinado a apresentar a finalidade da norma, não fez a delimitação específica dessa finalidade, nem esclareceu a necessidade de disponibilização dos dados ou sua adequação, vez que não dispôs como serão efetivamente utilizados, de modo que, assim, descumpriu o princípio do devido processo legal, conforme art. 5º, LIV, CF (STF, 2020).

Por fim, a relatora apontou que o art. 3º, I, II e §1º da Medida Provisória nº 954/2020, que dispõem, respectivamente, sobre o uso sigiloso dos dados disponibilizados, do atendimento exclusivo à finalidade trazida no art. 2º, §1º da norma (produção estatística oficial, com o objetivo de realizar entrevistas em caráter não presencial no âmbito de pesquisas domiciliares) e a vedação ao compartilhamento dos dados pelo IBGE não conferem a proteção necessária aos

dados pessoais contra seu vazamento, uso indevido ou invasão, e, portanto, aos direitos fundamentais mencionados (STF, 2020).

Por todas essas razões, decidiu-se pela suspensão da aplicabilidade da Medida Provisória nº 954/2020 até o julgamento das ADI's em comento (STF, 2020).

Ademais, existem regras que disciplinam o tratamento de dados pelo Poder Público, as quais estão disciplinadas nos artigos 23 a 30 da LGPD.

Na parte inicial do artigo 23, a LGPD dá a entender que as pessoas jurídicas de Direito Público que fazem o tratamento de dados pessoais são as mencionadas no parágrafo único do artigo 1º da Lei de Acesso à Informação, a saber:

Art. 1º (...)

Parágrafo único. Subordinam-se ao regime desta Lei:

I - os órgãos públicos integrantes da administração direta dos Poderes Executivo, Legislativo, incluindo as Cortes de Contas, e Judiciário e do Ministério Público;

II - as autarquias, as fundações públicas, as empresas públicas, as sociedades de economia mista e demais entidades controladas direta ou indiretamente pela União, Estados, Distrito Federal e Municípios.

Ou seja, o texto legal supratranscrito deixa claro que o tratamento de dados pessoais pelas pessoas jurídicas de Direito Público pode ser realizado tanto pela Administração Direta quanto pela Administração Indireta.

Durante esse tratamento, conforme dispõe a parte final do artigo 23 da LGPD, deverá ser buscado o atendimento da finalidade pública (o que consagra o princípio da impessoalidade), em prol do interesse público (consagração do princípio da supremacia do interesse público), executando-se as competências legais ou cumprindo as atribuições legais do interesse público (conforme o princípio da legalidade). De acordo com Tasso (2020), essa disposição complementa os ditames do artigo 7º, III da LGPD que se refere à autorização de tratamento de dados para a execução de políticas públicas.

Os incisos I e III do referido dispositivo legal, que seguem vigentes, impõem condições para que o tratamento dos dados pessoais pelo Poder Público seja realizado:

I - sejam informadas as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos;

(...)

III - seja indicado um encarregado quando realizarem operações de tratamento de dados pessoais, nos termos do art. 39 desta Lei. (Redação dada pela Lei nº 13.853, de 2019)

(...)

Tasso (2020) assevera que o inciso I consagra a necessidade de transparência no tratamento dos dados pessoais pelo Poder Público, e, por consequência, o já explicado princípio da transparência, que faz parte do grupo dos 10 princípios que regem a LGPD. Como a relação entre Poder Público e titular de dados é assimétrica, quando tal princípio é cumprido, este último sujeito passar a ter maior confiança no ente público controlador dos dados.

Ainda segundo Tasso (2020), quando o inciso I determina que, ao tratar os dados, o ente público deverá enunciar as hipóteses de tratamento, é perceptível o cumprimento do princípio da legalidade administrativa, ao passo que, quando a lei requisita que as informações sejam fornecidas de forma clara, atualizada e de fácil acesso, há concretização dos princípios da moralidade e da eficiência.

Por sua vez, quanto ao inciso III, o qual determina que deve haver indicação de um encarregado quando forem realizadas operações de tratamento de dados pessoais, Tasso (2020) aponta que o encarregado deverá ter um sólido conhecimento jurídico, para dar o correto valor ao direito personalíssimo sobre o qual posicionar-se-á como garantidor.

As outras disposições trazidas nos parágrafos do artigo 23 da LGPD são as seguintes:

§ 1º A autoridade nacional poderá dispor sobre as formas de publicidade das operações de tratamento.

§ 2º O disposto nesta Lei não dispensa as pessoas jurídicas mencionadas no caput deste artigo de instituir as autoridades de que trata a Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) .

§ 3º Os prazos e procedimentos para exercício dos direitos do titular perante o Poder Público observarão o disposto em legislação específica, em especial as disposições constantes da Lei nº 9.507, de 12 de novembro de 1997 (Lei do Habeas Data) , da Lei nº 9.784, de 29 de janeiro de 1999 (Lei Geral do Processo Administrativo) , e da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) .

§ 4º Os serviços notariais e de registro exercidos em caráter privado, por delegação do Poder Público, terão o mesmo tratamento dispensado às pessoas jurídicas referidas no caput deste artigo, nos termos desta Lei.

§ 5º Os órgãos notariais e de registro devem fornecer acesso aos dados por meio eletrônico para a administração pública, tendo em vista as finalidades de que trata o caput deste artigo.

Na sequência, o artigo 24 da LGPD versa sobre a igualdade de tratamento entre as pessoas jurídicas de direito privado particulares e as empresas públicas e sociedades de economia mista, que são submetidas ao artigo 173 da Constituição Federal.

Segundo Pinheiro (2018), a intenção dessa disposição legal foi diferenciar o tratamento das empresas públicas e sociedades de economia mista do tratamento de dados pessoais realizado nas instituições públicas, havendo preocupação com o atendimento de outras legislações, como a Lei de Acesso à Informação, em situações futuras.

O artigo 25 da LGPD dispõe o seguinte:

Art. 25. Os dados deverão ser mantidos em formato interoperável e estruturado para o uso compartilhado, com vistas à execução de políticas públicas, à prestação de serviços públicos, à descentralização da atividade pública e à disseminação e ao acesso das informações pelo público em geral.

De acordo com Pinheiro (2018, p. 65), as técnicas de manutenção dos dados em tratamento dispostas no artigo 25 da LGPD “são especificadas no caso das instituições públicas, de maneira que a sua estruturação e organização devem visar à execução das políticas públicas e à prestação de serviço”.

Tasso (2020) entende que tal regra se aplica tanto aos dados pessoais quanto aos dados sensíveis, devendo ser interpretada com base na máxima garantia dos direitos fundamentais garantidos pela LGPD.

O caput do artigo 26 da LGPD trata a respeito do uso compartilhado de dados pessoais pelo Poder Público, “o qual deve atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios de proteção de dados pessoais elencados no art. 6º desta Lei.”

Conforme Pinheiro (2018), tal dispositivo legal atribui ao Poder Público a incumbência de, ao mesmo tempo, garantir que o uso compartilhado de dados segue os propósitos especiais de execução de políticas públicas e, ao mesmo tempo, refletir se, apesar de as informações dos titulares de dados estarem disponíveis, há respeito a seus direitos individuais.

O §1º do artigo 26 da LGPD, por sua vez dispõe que, em regra, é vedado ao Poder Público transferir a entidades privadas os dados pessoais constantes nas bases de dados a que tiver acesso, com exceção dos 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 (inciso I), daqueles em que os dados forem acessíveis publicamente, observadas as disposições da LGPD (inciso III), quando houver previsão legal ou a transferência for respaldada em contratos, convênios ou instrumentos congêneres (inciso IV) ou 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 (inciso V).

Na sequência, o §2º complementa que deverá haver comunicação acerca dos contratos e convênios de que trata o parágrafo anterior.

O artigo 27 da LGPD trata sobre a necessidade de consentimento do titular quando houver comunicação ou uso compartilhado dos dados pessoais a pessoa jurídica, com exceção dos casos em que a dispensa de consentimento estiver prevista na lei (inciso I), nos casos de

uso compartilhado de dados (inciso II) e nas mesmas exceções previstas quanto a transferência de dados, conforme artigo 26, §1º da LGPD (inciso III).

A redação desse artigo, com razão, é criticada por Maciel:

Um leitor mais atento perceberá, que no final das contas, a transferência e o compartilhamento possuem os mesmos requisitos, numa redação absolutamente contraditória e de péssima técnica. Para piorar, dispensa consentimento, quando houver outra base legal e, naturalmente, o Poder Público trata dados majoritariamente com base em outras bases que não o consentimento, além de poder utilizar as exceções do art. 26. De quase nada serve essa disposição, se não para criar confusão, propositalmente talvez. É praticamente uma carta branca ao Poder Público. De qualquer modo, é importante lembrar que o Poder Público não está desincumbido de respeitar os demais princípios da lei, sobretudo os da finalidade, necessidade e adequação, podendo o ato ser considerado nulo se excessivo. (MACIEL, 2019, p. 52)

Compartilha-se, aqui, da opinião do autor supracitado, uma vez que é perceptível que, nesse ponto da LGPD, apesar da propagação da ideia de busca pela proteção do titular dos dados pessoais, muito vulnerável ao Poder Público, a redação mal trabalhada do artigo 27, não se sabe se de forma intencional, acabou por abrir uma brecha legal para que o ente estatal possa justificar seu acesso aos dados pessoais sem o consentimento do titular - que, como já visto, é requisito extremamente necessário ao tratamento de dados - em uma base legal diferente da LGPD, o que só não é mais catastrófico pelo fato de que o poder do ente estatal ainda não é ilimitado, devendo ele submeter-se aos demais princípios da LGPD e também do Direito Administrativo.

No mesmo sentido, asseveram Luciana Pedroso Xavier, Marília Pedroso Xavier e Mayara Guibor Spaler:

É crível que a criação e execução de muitas políticas públicas poderiam ser comprometidas pela falta de informações relevantes pelo Poder Público. No entanto, permitir que haja o compartilhamento de dados pessoais e sensíveis de forma livre e discricionária pela Administração Pública significa retirar a efetividade da legislação de proteção de dados. (XAVIER; XAVIER; SPALER, 2019, p. 288)

Por fim, os artigos 29 e 30 da LGPD estabelecem o seguinte:

Art. 29. A autoridade nacional poderá solicitar, a qualquer momento, aos órgãos e às entidades do poder público a realização de operações de tratamento de dados pessoais, informações específicas sobre o âmbito e a natureza dos dados e outros detalhes do tratamento realizado e poderá emitir parecer técnico complementar para garantir o cumprimento desta Lei. (Redação dada pela Lei nº 13.853, de 2019)

Art. 30. A autoridade nacional poderá estabelecer normas complementares para as atividades de comunicação e de uso compartilhado de dados pessoais.

Tais artigos versam sobre poderes que a Autoridade Nacional de Proteção de Dados tem para fiscalizar o tratamento de dados pessoais pelo Poder Público, de forma a garantir ao titular, como assevera Maciel (2019, p. 53), um “maior controle e segurança de seus dados pessoais.”

Outros poderes da Autoridade Nacional de Proteção de Dados estão nos artigos 31 e 32 da LGPD:

Art. 31. Quando houver infração a esta Lei em decorrência do tratamento de dados pessoais por órgãos públicos, a autoridade nacional poderá enviar informe com medidas cabíveis para fazer cessar a violação.

Art. 32. A autoridade nacional poderá solicitar a agentes do Poder Público a publicação de relatórios de impacto à proteção de dados pessoais e sugerir a adoção de padrões e de boas práticas para os tratamentos de dados pessoais pelo Poder Público.

Certamente, diante do desequilíbrio da relação entre o titular dos dados pessoais e o Poder Público, é difícil coibir a prática de abusos da Administração Pública no manejo de dados pessoais, cabendo à Autoridade Nacional de Proteção de Dados buscar equilibrar a situação, mediante fiscalização e aplicação de sanções em caso de tratamento de dados realizado em descumprimento à legislação, através de processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso, conforme dispõe o artigo 55-J, IV, da LGPD.

Além das sanções supracitadas também não se podem perder de vista as possibilidades de responsabilização segundo a LGPD e nem a hipótese de responsabilização civil quando for cometido algum dano contra o titular dos dados. Tais possibilidades serão discutidas no derradeiro capítulo do presente trabalho.

Mas antes de adentrar ao clímax da discussão, é necessário tecer considerações sobre o desequilibrado conflito entre o interesse público e o direito individual de proteção aos dados pessoais.

3.2 PROTEÇÃO AOS DADOS PESSOAIS *VERSUS* INTERESSE PÚBLICO

Conforme destacam Luciana Pedroso Xavier, Marília Pedroso Xavier e Mayara Guibor Spaler (2019), as prerrogativas advindas da supremacia do interesse público conferem ao Estado grande poder em relação aos cidadãos e organizações, de modo que, conforme consta no artigo 4º, III da LGPD, tal lei não deverá ser aplicada ao Poder Público para tratamento de dados envolvendo “segurança pública, defesa nacional, segurança do Estado e atividades de investigação e repressão de infrações penais” que serão tratados por lei específica prevendo medidas proporcionais e necessárias ao atendimento do interesse público.

De acordo com Marcelo Crespo (2021), essa supremacia, impulsionada pela obtenção massiva de dados pessoais pelo Estado, que deveria ser mais transparente no tratamento desses dados, concretiza-se em razão da obrigatoriedade de fornecimento dos dados pessoais ou dados

pessoais sensíveis pelos cidadãos para que tenham acesso a certos serviços, como por exemplo a aquisição de um imóvel ou veículo, atendimento em hospitais e a emissão de documentos.

Essa realidade demonstra a existência de grande vulnerabilidade e subordinação do titular dos dados perante ao Estado, posto que eventual postura negatória do indivíduo quanto ao fornecimento dessas informações pode criar travas quanto ao exercício de alguns de seus direitos individuais, como os citados no parágrafo antecedente.

O contexto de vulnerabilidade e subordinação trazido pode levar à crença de que, uma vez chocados o interesse individual, mais precisamente, a proteção dos dados pessoais, que é uma forma de concretização do direito à privacidade, com o interesse público, haverá sempre prevalência deste último sobre o primeiro.

Todavia, diante do que foi trazido no presente capítulo, o exercício de um mero raciocínio lógico permite perceber que nem sempre é assim, uma vez que, se o tratamento dos dados pessoais pelo Poder Público for realizado em descumprimento aos princípios que regem a Administração Pública ou aos princípios trazidos dentro da própria LGPD, prevalecerá o interesse individual, traduzido na proteção dos dados pessoais, uma vez que, em tal situação, o tratamento dos dados não poderá ser realizado.

Não se pode esquecer, também, que o direito à privacidade consagrado pela proteção aos dados pessoais na LGPD é derivado do princípio da dignidade humana, trazido no artigo 1º, III da Constituição Federal, que diz respeito, justamente, a possibilitação do desenvolvimento da personalidade do indivíduo (DIAS, 2015), de modo que, se houver choque entre o direito à privacidade e o interesse público, existe, na verdade, um choque de princípios (o da dignidade humana e o da supremacia do interesse público).

O conflito de princípios é diferente do conflito entre regras, posto que, enquanto este último pode ser resolvido pela exclusão de uma regra em favor da aplicação de outra (ALEXY, 2015), o primeiro deverá ser resolvido através da ponderação no caso concreto, ou seja, de acordo com as peculiaridades de cada situação, será escolhida a aplicação do princípio que for menos danoso, de modo que tal escolha não importará em invalidação do princípio preterido (DWORKIN, 2002).

Portanto, isso se aplica também ao embate entre o interesse público e a proteção aos dados pessoais, de modo que a supremacia do interesse público não é absoluta, devendo ser avaliado cada caso concreto para chegar-se à conclusão de qual interesse prevalecerá: o público ou o privado.

Ademais, eventuais violações cometidas pelo Estado quando do manejo dos dados pessoais não deverão passar impunes, havendo hipóteses de responsabilização segundo a LGPD

e, podendo ser defendida, também, a responsabilização civil do Poder Público em razão do indevido manejo dos dados pessoais, conforme será feito a seguir.

4. RESPONSABILIDADE CIVIL DO ESTADO PELO INDEVIDO MANEJO DE DADOS PESSOAIS

4.1 ASPECTOS GERAIS E PRESSUPOSTOS DA RESPONSABILIDADE CIVIL

Antes de demonstrar e justificar as razões pelas quais o Poder Público, quando causar danos ao titular de dados pessoais no tratamento destes, deverá ser responsabilizado civilmente, passando a ter o dever de indenizar tal sujeito, é importante esclarecer alguns dos principais aspectos do instituto da responsabilidade civil, bem como sua aplicação no Direito.

Segundo estudos de Gagliano e Pamplona Filho (2012), a responsabilidade jurídica tem relação com o ato danoso de certo indivíduo que, quando viola uma norma jurídica, pratica um ilícito, subordinando-se, por conseguinte, à obrigação de reparar o dano causado.

Sem perder o raciocínio, Gagliano e Pamplona Filho (2012) argumentam também que, no Direito Privado, a responsabilidade civil tem origem na agressão a um interesse particular e sujeita o agressor a compensar pecuniariamente a vítima, se houver impossibilidade de reestabelecimento da coisa ao estado anterior.

Como o presente trabalho visa defender uma das hipóteses de responsabilização civil estatal, sua ocorrência no Direito Público será estudada em tópico reservado.

A configuração da responsabilidade civil depende do preenchimento de certos requisitos trazidos pelo Código Civil.

Nos termos do artigo 186 desta lei, “aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito.”

Referindo-se ao dispositivo supra, Gonçalves (2012) esclarece que são quatro os pressupostos da responsabilidade civil, a saber, ação ou omissão, culpa ou dolo do agente, relação de causalidade e dano.

A ação (conduta positiva) ou a omissão (conduta negativa), nas palavras de Gagliano e Pamplona Filho (2012), originam-se da voluntariedade, ou seja, da liberdade de escolha do agente, inexistindo conduta sem manifestação de sua vontade.

Entretanto, Gagliano e Pamplona Filho (2012) apontam que, não obstante a responsabilidade civil decorra, em regra, de ato ilícito, há a possibilidade de o agente ser responsabilizado mesmo após atuação lícita, como por exemplo o caso da passagem forçada,

onde, nos termos do artigo 1.285 do Código Civil, o dono do prédio encravado sem acesso à via pública, nascente ou porto, pode constranger seu vizinho a dar-lhe passagem, por meio de pagamento indenização, sendo que, se esta não for acordada amigavelmente, poderá ser pleiteada via ação judicial, como no caso abaixo:

PASSAGEM FORÇADA – Imóvel encravado – Encravamento do imóvel pertencente ao autor demonstrado por laudo pericial – Passagem forçada bem reconhecida – Exegese do artigo 1.285 do Código Civil – Indenização devida pelo autor decorrente do texto legal – Ausência de prova de que o encravamento pode ser atribuído à apelada – Procedência em parte mantida – Recurso não provido. (TJ-SP - AC: 10004527920178260589 SP 1000452-79.2017.8.26.0589, Relator: Correia Lima, Data de Julgamento: 24/09/2020, 20ª Câmara de Direito Privado, Data de Publicação: 24/09/2020)

Ainda, ensina Gonçalves (2012), que a responsabilidade do agente pode advir de ato próprio (artigo 927 do Código Civil), de ato de terceiro sob sua guarda (artigo 932 do Código Civil) e, de forma objetiva, ou seja, independente de prova de culpa, por dano causado pelo animal (artigo 936 do Código Civil) ou coisa (artigos 937 e 938 do Código Civil) que lhe pertença.

Não pode ser esquecida, também, a disposição sobre responsabilidade civil objetiva no artigo 927, parágrafo único, do Código Civil, que como será visto no próximo tópico, é aplicável ao Poder Público:

Art. 927 (...)

Parágrafo único. Haverá obrigação de reparar o dano, independentemente de culpa, nos casos especificados em lei, ou quando a atividade normalmente desenvolvida pelo autor do dano implicar, por sua natureza, risco para os direitos de outrem.

No que se refere ao segundo pressuposto, Tartuce (2015) explica que a responsabilidade civil, com ou sem culpa, deve ser verificada com base na culpa em sentido amplo, a qual abrange tanto o dolo, quanto a culpa em sentido estrito.

O dolo, nas palavras de Tartuce (2015), decorre da violação ao dever jurídico com intenção de causar lesão a outrem, e se consubstancia nos termos “ação ou omissão voluntária”, do artigo 186 do Código Civil, de modo que, se verificado, enseja reparação total, nos termos do artigo 944, do Código Civil, equiparando-se, no direito privado, à culpa grave e não se enquadrando nas classificações do dolo estudadas no Direito Penal (dolo eventual, dolo não eventual e preterdolo).

Conforme definem Gagliano e Pamplona Filho (2012), a culpa em sentido estrito está associada ao desrespeito a uma norma jurídica pré-existente, e é composta por três elementos:

a voluntariedade da conduta do agente, a previsibilidade, ou seja, o prejuízo causado, proibido pelo Direito, deve ser previsível, e a violação de um dever de cuidado.

Para diferenciar a culpa do dolo, Cavalieri Filho (2005, p. 59, apud Tartuce, 2015, p. 385) assevera que “em suma, enquanto no dolo o agente quer a conduta e o resultado, a causa e a consequência, na culpa a vontade não vai além da ação ou omissão. O agente quer a conduta, não, porém, o resultado; quer a causa, mas não quer o efeito”, ou seja, na culpa, o agente não tem intenção de causar o resultado.

Conceitualmente, essa diferenciação tem grande importância, porém, Tartuce (2015, p. 385) explica que “para o Direito Civil não importa se o autor agiu com dolo ou culpa, sendo a consequência inicial a mesma, qual seja, a imputação do dever de reparação do dano ou indenização dos prejuízos”, muito embora argumente, por outro lado, com base nos artigos 944 e 945 do Código Civil, que a incidência do dolo ou da culpa pode ensejar em “redução equitativa da indenização.”

A culpa, segundo Gagliano e Pamplona Filho, pode ser manifestada de três formas:

- a) negligência — é a falta de observância do dever de cuidado, por omissão. Tal ocorre, por exemplo, quando o motorista causa grave acidente por não haver consertado a sua lanterna traseira, por desídia;
- b) imprudência — esta se caracteriza quando o agente culpado resolve enfrentar desnecessariamente o perigo. O sujeito, pois, atua contra as regras básicas de cautela. Caso do indivíduo que manda o seu filho menor alimentar um cão de guarda, expondo-o ao perigo;
- c) imperícia — esta forma de exteriorização da culpa decorre da falta de aptidão ou habilidade específica para a realização de uma atividade técnica ou científica. É o que acontece quando há o erro médico em uma cirurgia em que não se empregou corretamente a técnica de incisão ou quando o advogado deixa de interpor recurso que possibilitaria, segundo jurisprudência dominante, acolhimento da pretensão do seu cliente. (GAGLIANO; PAMPLONA FILHO, 2012, p. 205-206)

Além das formas de manifestação de culpa, Gonçalves traz outra forma de classificação para o elemento subjetivo:

A culpa pode ser, ainda, in eligendo: decorre da má escolha do representante, do preposto; in vigilando: decorre da ausência de fiscalização; in committendo: decorre de uma ação, de um ato positivo; in ommittendo: decorre de uma omissão, quando havia o dever de não se abster; in custodiendo: decorre da falta de cuidados na guarda de algum animal ou de algum objeto. (GONÇALVES, 2012, p. 52)

Outro detalhe sobre a culpa, segundo Gonçalves (2012) é que, apesar de, para a caracterização da responsabilidade civil, haver necessidade de verificação de culpa, consagrando a teoria subjetiva, verifica-se, em algumas situações, a responsabilidade objetiva,

onde a obrigação de reparar é determinada sem que seja analisada a existência de culpa, considerando-se a teoria do risco da atividade (artigo 927, parágrafo único do Código Civil):

RECURSO ESPECIAL. AÇÃO DE COMPENSAÇÃO DE DANOS MORAIS. ACIDENTE EM LINHA FÉRREA. TRANSPORTE DE PASSAGEIROS. RESPONSABILIDADE CIVIL OBJETIVA. ART. 734 DO CC/02. TEORIA DO RISCO CRIADO. ART. 927, PARÁGRAFO ÚNICO, DO CC/02. CONCRETIZAÇÃO DO RISCO EM DANO. EXCLUDENTES DA RESPONSABILIDADE. ROMPIMENTO DO NEXO CAUSAL. FORTUITOS INTERNOS. PADRÕES MÍNIMOS DE QUALIDADE NO EXERCÍCIO DA ATIVIDADE DE RISCO. FORTUITOS EXTERNOS. INOCORRÊNCIA. FATO DE TERCEIRO. CAUSA EXCLUSIVA DO DANO. NÃO DEMONSTRAÇÃO. EXONERAÇÃO DA RESPONSABILIDADE. HIPÓTESE CONCRETA. IMPOSSIBILIDADE. [...] **4. Na responsabilidade civil objetiva, os danos deixam de ser considerados acontecimentos extraordinários, ocorrências inesperadas e atribuíveis unicamente à fatalidade ou à conduta (necessariamente no mínimo) culposa de alguém, para se tornarem consequências, na medida do possível, previsíveis e até mesmo naturais do exercício de atividades inerentemente geradoras de perigo, cujos danos demandam, por imperativo de solidariedade e justiça social, a adequada reparação. 5. Para a responsabilidade objetiva da teoria do risco criado, adotada pelo art. 927, parágrafo único, do CC/02, o dever de reparar exsurge da materialização do risco - da inerente e inexorável potencialidade de qualquer atividade lesionar interesses alheios - em um dano; da conversão do perigo genérico e abstrato em um prejuízo concreto e individual. Assim, o exercício de uma atividade obriga a reparar um dano, não na medida em que seja culposa (ou dolosa), porém na medida em que tenha sido causal. a fixação de um quadrante à luz das condições mínimas esperadas do exercício profissional, que deve ser essencialmente dinâmico, e dentro dos quais a concretização dos riscos em dano é atribuível àquele que exerce a atividade. [...]** (STJ - REsp: 1786722 SP 2018/0258668-4, Relator: Ministra NANCY ANDRIGHI, Data de Julgamento: 09/06/2020, T3 - TERCEIRA TURMA, Data de Publicação: DJe 12/06/2020, grifo nosso)

O terceiro pressuposto da responsabilidade civil é o nexo de causalidade, que, de acordo com Gonçalves (2012, p. 52) é a “relação de causa e efeito entre a ação ou omissão do agente e o dano verificado”.

Destarte, como esclarecem Gagliano e Pamplona Filho (2012), o agente somente responderá civilmente se sua conduta for a causa do dano experimentado por um terceiro.

O último pressuposto da responsabilidade civil é o dano.

A respeito desse pressuposto, Gonçalves (2012) aponta que, apesar de ser possível atribuir responsabilidade civil sem incidência de culpa, o mesmo não pode ser feito com relação ao dano, de forma que, sem este último elemento, é impossível falar-se em dever de indenizar.

Complementando tal raciocínio, Gagliano e Pamplona Filho (2012) asseveram que o interesse na responsabilização existe se o dano perdurar no momento da propositura da ação, não havendo pretensão se já tiver se verificado sua reparação.

Diante do papel de protagonismo que o dano exerce na verificação da responsabilidade civil, torna-se importante verificar qual a sua definição segundo os estudiosos do Direito.

Segundo Gagliano e Pamplona Filho (2012, p. 88), o dano é a “*lesão a um interesse jurídico tutelado — patrimonial ou não —, causado por ação ou omissão do sujeito infrator* (grifo dos autores)”.

Por sua vez, Venosa (2013, p. 38) aponta que o dano “é o prejuízo individual ou coletivo, moral ou material, ou melhor, econômico ou não econômico”, advém da injusta lesão a interesse, deve ser atual e certo, excluindo-se, em regra, os danos hipotéticos, e se materializa com a apuração do prejuízo ao qual foi submetido o indivíduo lesado.

Como quase toda regra possui uma exceção, Venosa (2013) argumenta que, a perda de uma chance, relacionada à frustração da percepção de ganhos pela vítima da lesão, permite que seja pleiteada indenização baseada em dano incerto, projetado por ocasião da definição do quantum indenizatório e condicionado a termo, salientando que a situação da perda importa em lesão patrimonial, e não somente de uma expectativa.

De acordo com Gagliano e Pamplona Filho (2012, p. 92) há duas espécies principais de dano: o patrimonial ou material e o moral, sendo que a primeira espécie é a “lesão aos bens e direitos economicamente apreciáveis do seu titular”.

No mesmo sentido, Tartuce (2015, p. 394) pontua que “os danos patrimoniais ou materiais constituem prejuízos ou perdas que atingem o patrimônio corpóreo de alguém.”

Ademais, Venosa (2013) ensina que a quantificação dos danos patrimoniais, se originados de inadimplemento contratual, será realizada de acordo com o valor do contrato, sem exclusão das cláusulas penais que possam ser aplicadas em razão de tal situação. Porém, se a responsabilidade civil for extracontratual, deverá haver avaliação dos prejuízos no caso concreto, conforme determinado pelo artigo 946 do Código Civil.

Tomando por base o artigo 402 do Código Civil, Gagliano e Pamplona Filho (2012) dividem os danos materiais em emergentes, os quais consistem nos prejuízos efetivamente experimentados pela vítima, e nos lucros cessantes, ou seja, aquilo que tal pessoa deixou de receber por causa do dano sofrido.

O dano moral, tem existência e possibilidade de reparação positivadas no artigo 5º, V e X da Constituição Federal e na parte final do artigo 186 do Código Civil:

Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:

[...]

V - é assegurado o direito de resposta, proporcional ao agravo, além da indenização por dano material, moral ou à imagem;

[...]

X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;
[...]

Art. 186. Aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, **ainda que exclusivamente moral**, comete ato ilícito. (grifo nosso)

Considerando o disposto no artigo 5º, inciso X, da Constituição Federal, Gagliano e Pamplona Filho (2012) conceituam a lesão moral como aquela que fere os direitos da personalidade, a saber, a intimidade, a vida privada, a honra e a imagem da vítima.

Num português mais claro, Gonçalves (2012) aduz que o dano moral lesiona o vitimado como pessoa, acarretando-lhe sentimentos de dor, vexame, tristeza e humilhação.

Sobre a dimensão do dano moral, Silvio Venosa adverte:

Nesse campo, o prejuízo transita pelo imponderável, daí porque aumentam as dificuldades de se estabelecer a justa recompensa pelo dano. Em muitas situações, cuida-se de indenizar o inefável. Não é também qualquer dissabor comezinho da vida que pode acarretar a indenização. Aqui, também é importante o critério objetivo do homem médio, o *bonus pater familias*: não se levará em conta o psiquismo do homem excessivamente sensível, que se aborrece com fatos diuturnos da vida, nem o homem de pouca ou nenhuma sensibilidade, capaz de resistir sempre às rudezas do destino. Nesse campo, não há fórmulas seguras para auxiliar o juiz. Cabe ao magistrado sentir em cada caso o pulsar da sociedade que o cerca. O sofrimento como contraposição reflexa da alegria é uma constante do comportamento humano universal. (VENOSA, 2013, p. 47)

Portanto, o posicionamento do autor supracitado deixa claro que nem toda situação que chateia o ser humano enseja a reparação por danos morais, posto que se assim fosse, tal instituto seria banalizado, devendo ser indenizadas somente as ocorrências que afetem efetivamente os direitos da personalidade da vítima.

São inúmeros os casos onde o magistrado entende que a lesão moral alegada pelo requerente se trata de mero aborrecimento, ao qual o homem médio está sujeito em seu cotidiano, como o exemplo abaixo:

AGRAVO EM RECURSO ESPECIAL Nº 1.818.335 - MS (2021/0021266-4)
DECISÃO Cuida-se de agravo apresentado por JULIANA BUENO DE CASTRO e OUTROS contra a decisão que não admitiu seu recurso especial. O apelo nobre, fundamentado no artigo 105, inciso III, alínea a da CF/88, visa reformar acórdão proferido pelo TRIBUNAL DE JUSTIÇA DO ESTADO DO MATO GROSSO DO SUL, assim resumido: RECURSO DE APELAÇÃO - AÇÃO DE INDENIZAÇÃO POR DANOS MORAIS - REALOCAÇÃO DE VOO POR PROBLEMAS TÉCNICOS - AUMENTO DE 5 HORAS NO TEMPO DA CONEXÃO - MERO ABORRECIMENTO - DANO MORAL NÃO CONFIGURADO - SENTENÇA MANTIDA RECURSO CONHECIDO E IMPROVIDO. O aumento do tempo de

conexão do voo não é capaz de gerar repercussões negativas à esfera jurídica do sujeito, não constituindo, por si só, causa satisfativa a fim de gerar dano moral indenizável, notadamente diante da ausência de danos concretos ao consumidor a partir de situação comum do cotidiano, ensejadora de mero aborrecimento. Recurso conhecido e improvido. [...] (STJ - AREsp: 1818335 MS 2021/0021266-4, Relator: Ministro HUMBERTO MARTINS, Data de Publicação: DJ 25/02/2021)

Uma característica interessante a respeito dos danos morais é que, nas palavras de Gonçalves (2012), em regra, tal lesão não precisa ser provada, posto que se concretiza dentro da personalidade da vítima, gozando de presunção absoluta, exceto em casos específicos, como o descumprimento contratual.

Enfim, sobre a natureza jurídica da indenização por dano moral, Gonçalves (2012) assevera que prevalece o entendimento de que esta possui um duplo papel: o de compensar ou atenuar o sofrimento da vítima em razão da lesão sofrida e o de punir o ofensor, desestimulando-o de repetir a conduta causadora do dano extrapatrimonial.

Após a exposição dos principais aspectos sobre os elementos da responsabilidade civil, é chegado o momento de entender como se dá no âmbito do Poder Público, para depois descobrir se é viável sua aplicação quando o ente público fizer uso indevido de dados pessoais.

4.2 RESPONSABILIDADE CIVIL DO ESTADO E TEORIA DO RISCO ADMINISTRATIVO

Como visto, para que haja configuração da responsabilidade civil objetiva, é dispensada a averiguação se houve culpa do ofensor. Para tanto, conforme Mello (2015), basta que haja nexo de causalidade entre a conduta do agente e o dano causado à vítima

A aplicação da responsabilidade civil objetiva em face do Estado, de acordo com Carvalho Filho (2020), consagrou-se em razão da disparidade jurídica, econômica e política entre a Administração Pública e o administrado, de modo que seria injusto que este último, diante do dano causado pela atividade estatal, necessitasse de demasiado empenho para comprovar seu direito de ser indenizado.

Sendo assim, Carvalho Filho (2020) aponta que começou a ser defendida a tese de que, por ser muito poderoso, o Estado deveria ter de lidar com um risco natural pelo exercício de suas inúmeras atividades, ou seja, quanto maior o poder, maior o risco. Tal teoria, segundo ele, é chamada de “Teoria do Risco Administrativo” e é a base da responsabilidade civil objetiva do Estado.

No ordenamento jurídico brasileiro, tal teoria se consagrou nos artigos 37, §6º da Constituição Federal e 43 do Código Civil, sendo a regra no que se refere à responsabilidade civil estatal:

Art. 37, CF. A administração pública direta e indireta de qualquer dos Poderes da União, dos Estados, do Distrito Federal e dos Municípios obedecerá aos princípios de legalidade, impessoalidade, moralidade, publicidade e eficiência e, também, ao seguinte:

(...)

§ 6º As pessoas jurídicas de direito público e as de direito privado prestadoras de serviços públicos 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. (grifo nosso)

Art. 43. As pessoas jurídicas de direito público interno são civilmente responsáveis por atos dos seus agentes que nessa qualidade causem danos a terceiros, ressalvado direito regressivo contra os causadores do dano, se houver, por parte destes, culpa ou dolo.

Os textos legais em comento permitem perceber, que uma vez causado o dano, não importa se o Estado teve culpa/dolo ou não, deverá responder, sendo resguardado a ele apenas o direito de regresso contra o verdadeiro causador do dano, se comprovar culpa/dolo deste último.

Segundo Meirelles (2016), para a teoria do risco administrativo, bastará a ocorrência de fato do serviço que ocasione dano ao administrado para que seja imposta ao Estado a obrigação de indenizar. O autor ressalva, contudo, que tal teoria abre espaço para que o Estado consiga a exclusão ou diminuição da obrigação de indenizar se comprovar que o dano se deu por culpa exclusiva da vítima, de terceiro, por conta de caso fortuito ou de força maior.

Ainda conforme Meirelles (2016), o fato de poderem incidir excludentes de responsabilidade sobre o fato do serviço estatal diferencia a teoria do risco administrativo da teoria do risco integral, segundo a qual qualquer lesão causada pelo Estado ao administrado deverá ser indenizada, ainda que esta resulte de dolo ou culpa da vítima. O autor salienta, por fim, que tal teoria foi rejeitada no ordenamento jurídico justamente por sua radicalidade, prevalecendo sobre ela a teoria do risco administrativo, que é mais amena.

Como foi visto, a redação do artigo 37, §6º da Constituição Federal coloca como sujeitos responsáveis pelos danos causados pelo Estado a terceiros tanto as pessoas jurídicas de direito público (incluídos os membros da Administração direta e da indireta) quanto as pessoas jurídicas de direito privado prestadoras de serviços públicos.

Nas palavras de Carvalho Filho (2020), a inclusão dessa segunda categoria de sujeitos se deu com a intenção de igualar as pessoas jurídicas de direito público àquelas que, embora

conservem sua personalidade jurídica de direito privado, prestam, por delegação estatal, serviços, cuja responsabilidade seria da Administração Pública, de modo que, sendo o serviço público, não seria justo dificultar a reparação aos prejuízos sofridos pelos administrados.

De acordo com Mello (2015), são dois os fundamentos da responsabilidade civil objetiva do Poder Público, a depender do tipo de ato praticado. Se houver um comportamento ilícito, comissivo ou omissivo, a responsabilidade deriva do princípio da legalidade. Por sua vez, se houver comportamento lícito, mesmo que o Estado não seja o autor do dano, sua responsabilidade advém da necessidade de garantir uma repartição equilibrada dos ônus decorrentes do ato ou efeito lesivo, razão pela qual, nesse caso, o fundamento é o princípio da igualdade.

Entendidos os principais aspectos acerca da responsabilidade civil do Estado, finalmente chegou o momento de verificar sua aplicabilidade em face do Poder Público quando este manejar indevidamente os dados pessoais dos administrados.

4.3 RESPONSABILIDADE CIVIL DO ESTADO PELOS DANOS CAUSADOS POR SEUS AGENTES ATRAVÉS DO INDEVIDO MANEJO DE DADOS PESSOAIS SEGUNDO A LGPD

Na Seção III do Capítulo VI da Lei Geral de Proteção de Dados Pessoais (artigos 42 a 45), foi reservado espaço para a atribuição de responsabilidade civil aos controladores ou operadores de dados pessoais que cometerem erros ou excessos que ocasionem danos ao titular dos dados pessoais.

O artigo 42 da referida lei tem a seguinte redação:

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.

§ 1º A fim de assegurar a efetiva indenização ao titular dos dados:

I - o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador equipara-se ao controlador, salvo nos casos de exclusão previstos no art. 43 desta Lei;

II - os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente, salvo nos casos de exclusão previstos no art. 43 desta Lei.

§ 2º O juiz, no processo civil, poderá inverter o ônus da prova a favor do titular dos dados quando, a seu juízo, for verossímil a alegação, houver hipossuficiência para fins de produção de prova ou quando a produção de prova pelo titular resultar-lhe excessivamente onerosa.

§ 3º As ações de reparação por danos coletivos que tenham por objeto a responsabilização nos termos do caput deste artigo podem ser exercidas coletivamente em juízo, observado o disposto na legislação pertinente.

§ 4º Aquele que reparar o dano ao titular tem direito de regresso contra os demais responsáveis, na medida de sua participação no evento danoso. (grifo nosso)

Como se vê, a LGPD não prevê expressamente se a responsabilização civil disposta no caput do seu artigo 42 se aplica também ao Estado enquanto agente de tratamento de dados, o que poderia causar dúvidas quanto à sua aplicabilidade contra os entes públicos.

Até porque, como visto, existe uma grande vulnerabilidade na relação jurídica entre o administrado e a Administração Pública, posto que esta última possui vastos poderes aptos a controlar o destino de quem se opõe à sua vontade, podendo inclusive sobrepor-se a ela, como destaca Bruna Simões, doutora em Direito pela PUC-SP:

Note-se ainda que no caso do Poder Público, em muitas situações, o fornecimento dos dados é obrigatório para acesso ao serviço, de maneira que, nestes casos, não há consentimento do titular, na medida em que a negativa do dado pessoal implica em não acessar o serviço. (SIMÕES, 2021, on-line)

Ora, ao impor ao titular a abusiva obrigação de fornecer os dados pessoais para ter acesso a determinado serviço, o Poder Público passa por cima do consentimento de tal sujeito, violando este que é um dos principais requisitos para o tratamento de dados pessoais.

Obviamente, a violação ao consentimento, por reflexo, consiste em violação à LGPD, o que, por si só, já encerraria a discussão sobre a possibilidade ou não de a pessoa jurídica de Direito Público ser responsabilizada civilmente pelo uso indevido de dados.

Todavia, analisando de forma sistemática a LGPD, fica ainda mais evidente que, quando for o caso, a responsabilidade civil pelo manejo incorreto de dados pessoais deverá recair sobre o Poder Público.

Isso porque, como se viu, a redação do artigo 42 da LGPD, sem abrir exceções ou excluir tratadores de dados, dispõe que, se o controlador ou operador de dados violar a LGPD causando dano a outrem, deverá responder civilmente por tal fato.

Assim sendo, se entre seus artigos 23 e 30 a LGPD retrata o tratamento de dados pelo Poder Público, obviamente, este poderá ocupar a posição de controlador ou operador, razão pela qual está sujeito a todas as regras da LGPD, inclusive as de responsabilidade civil por danos causados.

Incontroverso, portanto, que, se causar danos no tratamento de dados pessoais, o Poder Público deverá ser responsabilizado civilmente.

Todavia, como destaca Marcos da Silva Gomes Bruno (2020), a LGPD não é clara sobre qual tipo de responsabilidade civil (subjéitiva ou objéitiva) deverá ser aplicada aos sujeitos que se enquadrem no disposto em seu artigo 42. O autor destaca, porém, que, como a regra geral, em se tratando de responsabilidade civil, é a aplicação da responsabilidade subjéitiva, sendo a responsabilidade objéitiva aplicada apenas em situações excepcionais, como já foi visto, não deve ser diferente quanto à LGPD, prevalecendo, portanto, a regra geral.

Entretanto, levando em conta que o Poder Público responde à teoria do risco administrativo, a ele se aplica uma das situações excepcionais mencionadas pelo autor supracitado, razão pela qual se defende aqui que a responsabilidade civil do Estado pelo indevido manejo de dados é objéitiva.

O artigo 43 da LGPD, por sua vez, dispõe o seguinte:

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.

Como também foi visto, a Teoria do Risco Administrativo permite ao Estado que afaste sua responsabilidade civil se comprovar que o dano foi causado por terceiro, que ocorreu caso fortuito ou de força maior ou que houve culpa exclusiva da vítima, de forma que é possível defender a exclusão da responsabilidade estatal se preenchidos os requisitos dos incisos I e III do artigo 43 da LGPD.

Bruna Simões (2021) defende, porém, que a excludente de responsabilidade disposta no inciso II do artigo 43 da LGPD não se aplica ao Poder Público como controlador ou operador dos dados pessoais, eis que, por ser a responsabilidade estatal objéitiva nesse caso, tendo existido o dano, não há que se falar em afastamento da responsabilidade por não violação da legislação.

Diante da possibilidade de o Estado ser responsabilizado civilmente mesmo quando comete ato lícito, é possível perceber que o argumento supra faz sentido.

Ademais, Bruna Simões (2021) defende que, já que a LGPD não estabelece os patamares indenizatórios da responsabilidade civil por uso indevido de dados, poderão ser utilizados, no caso concreto, o artigo 944 do Código Civil (o qual determina que a indenização é medida pela extensão do dano) e os artigos 50 e 52, §1º e incisos da LGPD, que trazem, respectivamente, disposições sobre boas práticas e governança e critérios para definição de sanções.

Para que não surjam dúvidas sobre qual tipo de tratamento de dados pessoais é irregular, demandando responsabilização civil do controlador ou operador pelos danos que causar, o artigo 44 da LGPD dispõe o seguinte:

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.

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.

Já há, inclusive, julgados condenando o Estado pelo uso indevido de dados do administrado, como no caso abaixo, que ainda não mencionava a LGPD, pois quando iniciada a lide, tal lei não estava em vigor, mas tem forte ligação com as disposições dessa lei:

CIVIL E PROCESSUAL CIVIL. RESPONSABILIDADE CIVIL. UNIÃO. DANO MORAL. INSTAURAÇÃO DE INQUÉRITO POLICIAL. HIPÓTESE DE HOMONÍMIA. CONDUTA DESIDIOSA DO ESTADO. USO INDEVIDO DO NOME E DE DADOS PESSOAIS PERTENCENTES AO DEMANDANTE. PROCEDIMENTO INVESTIGATIVO REGISTRADO EM CERTIDÃO PÚBLICA. REPARAÇÃO DO EVENTO DANOSO. CABIMENTO. APELAÇÃO PARCIALMENTE PROVIDA. PEDIDO JULGADO PROCEDENTE EM PARTE. 1. O apelante afirma ter sofrido dano moral, em razão de haver sido instaurado inquérito policial envolvendo seu nome e o respectivo Cadastro de Pessoas Físicas (CPF), quando, na realidade, o envolvido com os fatos delituosos objeto da investigação era pessoa com nome semelhante ao seu. 2. Compulsando os autos, é possível verificar que a Certidão de Distribuição Regional (Ações e Execuções), emitida pela Justiça Federal da Seção Judiciária do Pará, na data de 12.05.2009, registra, em nome do apelante, a existência do Inquérito Policial n. 2008.39.00.000.283-0, em trâmite, na época, junto à 3ª Vara Federal. **3. Na hipótese está satisfatoriamente configurado erro da Administração, que deu início a um procedimento investigatório indicando não apenas o nome do apelante, mas também, dados pessoais como o número do CPF, demonstrando evidente desídia, ao deixar de adotar as cautelas necessárias e exigíveis, em tais casos, para que a pessoa, cuja desventura seja possuir nome idêntico ao do verdadeiro investigado, não venha a passar por incômodos semelhantes aos experimentados pelo autor.** 4. O abalo experimentado, na hipótese em exame, vai além do mero aborrecimento, diante do ônus que o Estado acabou por impor ao apelante, de comprovar não ter tido nenhum envolvimento com a conduta criminosa objeto da investigação. 5. Na hipótese, o montante de R\$ 5.000,00 (cinco mil reais), diante das circunstâncias do caso, mostra-se razoável para reparar o gravame sofrido, levando-se em conta que, de fato, não ficou demonstrada a alegada detenção por 5 (cinco) horas na sede da Polícia Federal, ônus que competia ao autor, nos termos do art. 373, inciso I, do Código de Processo Civil (CPC) de 2015. 6. Juros de mora fixados com base no índice de remuneração da caderneta de poupança. 7. A correção monetária deve ser levada a efeito mediante a aplicação do IPCA-E, a partir da data do arbitramento. 8. A incidência dos juros de mora, na espécie, deve ser feita em consonância com os ditames da Súmula n. 54 do Superior Tribunal de Justiça, a partir do evento danoso. 9. Apelação parcialmente provida. Pedido julgado procedente, em parte. (TRF 1 - 00002267220124013701, Relator: Daniel Paes Ribeiro, Data de Julgamento: 08/04/2019, 6ª Turma, Data de Publicação no DJF: 26/04/2019) (grifo nosso)

Destarte, diante de tudo o que foi exposto, é possível concluir que é forte a tendência de crescimento da aplicação da LGPD, lei relativamente nova, a casos de responsabilidade civil por uso indevido de dados, mesmo que neles esteja no polo passivo o Poder Público, cuja relação com o administrado, como visto, é extremamente desequilibrada.

CONCLUSÃO

O escopo da presente pesquisa foi o de apresentar um problema que afeta milhões de brasileiros em se tratando do tratamento de dados pessoais: a violação de seu direito à privacidade pelo Estado, através do uso indevido de tais informações, oferecendo-se uma solução apta a diminuir os prejuízos desta situação ao particular, bem como ligar o sinal de alerta ao Poder Público acerca dos cuidados que deve ter quando manejar dados pessoais alheios.

Como o problema está ligado ao tratamento de dados pessoais, tornou-se importante, em primeiro lugar, trazer a relação entre a proteção dos dados pessoais e o direito à privacidade, trazendo, em seguida, contornos históricos sobre a proteção dos dados pessoais no Brasil antes da LGPD e, por fim, trazer os principais aspectos a respeito da referida lei.

Na sequência, foi reservado capítulo especial para explicar alguns aspectos específicos da LGPD, tais quais quem são os agentes de tratamento de dados e quais suas obrigações, quais os tipos de dados tutelados pela lei, como se dá o término do tratamento de dados e, por fim, quais os direitos do titular dos dados pessoais.

Aproximando-se da apresentação do problema e de sua solução, buscou-se estabelecer como se dá a relação do Poder Público com o sistema de proteção de dados, esclarecendo-se detalhes sobre a atividade da Administração Pública e os princípios aos quais essa se submete, bem como demonstrando como é a atuação pública em relação ao tratamento de dados, sendo finalizada essa parte com a discussão acerca do choque do princípio da supremacia do interesse público com a proteção de dados pessoais, forma de manifestação do direito à privacidade, que consiste em um dos direitos da personalidade.

Nesse momento, foi desenvolvida argumentação demonstrando o porquê de a relação entre a Administração Pública e o administrado ser tão desequilibrada, ocasionando em violações injustas do primeiro a direitos do último, como quando o Estado se utiliza de dados pessoais do particular mesmo sem sua autorização, passando por cima do consentimento, uma das principais bases do tratamento de dados.

Apresentado o problema da violação de direitos pessoais pelo Estado, mais especificamente no que se refere ao desrespeito à privacidade e ao direito de o titular de dados de buscar sua proteção, passou a ser retratado o instituto da responsabilidade civil.

Primeiramente, foram trazidos os principais aspectos de tal instituto no Direito Civil, matéria que o estuda com afinco, para, na sequência, estudar como se dá sua aplicação no Direito Público.

Como se viu, quando se fala em responsabilidade civil do Estado, este responde à teoria do risco administrativo, que atribui a tal figura a responsabilidade civil objetiva, ou seja, para que nasça a obrigação de indenizar, basta o nexo causal entre a conduta estatal e o dano sofrido pelo particular, não havendo que se falar em análise acerca da culpa para que haja a condenação estatal.

Ao final do trabalho, foi explicado como é aplicada a responsabilidade civil segundo a LGPD, tendo sido demonstrado que, como o Estado se submete a tal lei e pode atuar na posição de agente de tratamento de dados, pode ser submetido à responsabilidade civil quando violar os direitos do titular dos dados pessoais.

Por tais razões, é possível concluir que, ainda que exista vulnerabilidade e desequilíbrio na relação entre a Administração Pública e particular, e que se imagine ser difícil a concretização da hipótese defendida no trabalho, se o Estado abusar de seu imenso rol de direitos quando ficar responsável por cuidar dos dados pessoais alheios, deverá sofrer as consequências pelos danos causados, através de sua responsabilização civil, que servirá de exemplo aos particulares e incentivará o Poder Público a ser mais zeloso quanto ao tratamento de dados do particular.

REFERÊNCIAS

ALEXY, Robert. **Teoria dos direitos fundamentais**. 2. ed. São Paulo: Malheiros, 2015.

ARAÚJO, Luiz Alberto David; NUNES JÚNIOR, Vidal Serrano. **Curso de Direito Constitucional**. 20. ed. São Paulo: Verbatim, 2016.

BASTOS, Elísio Augusto Velloso; PANTOJA, Tiago Luis Souza; SANTOS, Sérgio Henrique Costa Silva dos. OS IMPACTOS DAS NOVAS TECNOLOGIAS DA INFORMAÇÃO E COMUNICAÇÃO NO DIREITO FUNDAMENTAL À PRIVACIDADE / THE IMPACTS OF NEW INFORMATION AND COMMUNICATION TECHNOLOGIES IN THE FUNDAMENTAL RIGHT TO PRIVACY. **Brazilian Journal Of Development**, [S.L.], v. 7, n. 3, p. 29247-29267, 2021. Brazilian Journal of Development. Disponível em: <<https://www.brazilianjournals.com/index.php/BRJD/article/view/26840/21237>> Acesso em: 15 abr. 2022.

BRASIL. **Constituição Federal da República Federativa do Brasil de 1988**. Brasília, DF, 05 out. 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm> Acesso em: 10 mar. 2022.

_____. Institui a Política de Privacidade e de Proteção de Dados Pessoais no âmbito do Supremo Tribunal Federal. **Resolução nº 759, do Supremo Tribunal Federal**. Brasília, DF, 07 jan. 2022. Disponível em: <<https://www.stf.jus.br/arquivo/norma/resolucao759-2021.pdf>> Acesso em: 07 maio 2022.

_____. **Código Civil**. Lei nº 10.406, de 10 de janeiro de 2002. Institui o Código Civil. Brasília, DF, 11 jan. 2002. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/2002/110406compilada.htm> Acesso em: 15 mar. 2022.

_____. **Código de defesa do consumidor**. Lei nº 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. 11 set. 1990. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/18078compilado.htm> Acesso em 11 abr. 2022.

_____. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Brasília, DF, Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm> Acesso em: 11 mar. 2022.

_____. Lei nº 12.527, de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. **Lei de Acesso à Informação**. Brasília, DF, Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/112527.htm> Acesso em 15 abr. 2022.

_____. Superior Tribunal de Justiça. Recurso Especial. Ação de Compensação de Danos Morais. Acidente em Linha Férrea. Transporte de Passageiros. Responsabilidade Civil

Objetiva. Art. 734 do Cc/02. Teoria do Risco Criado. Art. 927, Parágrafo Único, do Cc/02. Concretização do Risco em Dano. Excludentes da Responsabilidade. Rompimento do Nexo Causal. Fortuitos Internos. Padrões Mínimos de Qualidade no Exercício da Atividade de Risco. Fortuitos Externos. Inocorrência. Fato de Terceiro. Causa Exclusiva do Dano. Não Demonstração. Exoneração da Responsabilidade. Hipótese Concreta. Impossibilidade. nº 1.786.722. Relator: Ministra Nancy Andrichi. Brasília, DF, 09 de junho de 2020. **Diário de Justiça Eletrônico**. Brasília, 12 jun. 2020. Disponível em: <<https://stj.jusbrasil.com.br/jurisprudencia/859838634/recurso-especial-resp-1786722-sp-2018-0258668-4/inteiro-teor-859838635>> Acesso em: 20 abr. 2022.

_____. Superior Tribunal de Justiça. Agravo em Recurso Especial Nº 1.818.335 - Ms (2021/0021266-4) Decisão nº 1.818.335. Relator: Ministro Humberto Martins. Brasília, DF, 24 de fevereiro de 2021. **Diário de Justiça Eletrônico**. Brasília, 25 fev. 2021. Disponível em: <<https://stj.jusbrasil.com.br/jurisprudencia/1172121331/agravo-em-recurso-especial-aresp-1818335-ms-2021-0021266-4/decisao-monocratica-1172121341>> Acesso em: 04 maio 2022.

_____. **Medida Provisória nº 954, de 17 de abril de 2020**. Dispõe sobre o compartilhamento de dados por empresas de telecomunicações prestadoras de Serviço Telefônico Fixo Comutado e de Serviço Móvel Pessoal com a Fundação Instituto Brasileiro de Geografia e Estatística, para fins de suporte à produção estatística oficial durante a situação de emergência de saúde pública de importância internacional decorrente do coronavírus (covid-19), de que trata a Lei nº 13.979, de 6 de fevereiro de 2020. Brasília, DF, 17 abr. 2020. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/mpv/mpv954.htm> Acesso em: 18 maio 2020.

_____. Supremo Tribunal Federal. Medida Cautelar na Adi nº 6387. Relator: Ministra Rosa Weber. Brasília, DF, 07 de maio de 2020. **Diário Oficial da União**. Brasília, 12 nov. 2020. Disponível em: <https://jurisprudencia.stf.jus.br/pages/search?classeNumeroIncidente=%22ADI%206387%22&base=acordaos&sinonimo=true&plural=true&page=1&pageSize=10&sort=_score&sortBy=desc&isAdvanced=true>. Acesso em: 18 maio 2022.

BRUNO, Marcos Gomes da Silva. Capítulo VI: dos agentes de tratamento de dados pessoais. In: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. **LGPD: lei geral de proteção de dados comentada**. 2. ed. São Paulo: Thomson Reuters Brasil, 2020. Cap. 6. p. 345-371.

CARVALHO FILHO, José dos Santos. **Manual de Direito Administrativo**. 34. ed. São Paulo: Atlas, 2020.

CRESPO, Marcelo. Proteção de dados pessoais e o Poder Público: noções essenciais. In: CRAVO, Daniela Copetti; CUNDA, Daniela Zago Gonçalves da; RAMOS, Rafael. **Lei Geral de Proteção de Dados e o Poder Público**. Porto Alegre: Escola Superior de Gestão e Controle Francisco Juruena; Centro de Estudos de Direito Municipal, 2021. Cap. 1. p. 16-28. Disponível em: <https://lproweb.procempa.com.br/pmpa/prefpoa/pgm/usu_doc/ebook_lgpd_e_poder_publico_23052021.pdf> Acesso em: 06 maio 2022.

DIAS, Maria Berenice. **Manual de Direito das Famílias**. 10. ed. São Paulo: Editora Revista dos Tribunais, 2015.

DISTRITO FEDERAL. Tribunal Regional Federal da 1ª Região. Civil e Processual Civil. Responsabilidade Civil. União. Dano Moral. Instauração de Inquérito Policial. Hipótese de Homonímia. Conduta Desidiosa do Estado. Uso Indevido do Nome e de Dados Pessoais Pertencentes Ao Demandante. Procedimento Investigativo Registrado em Certidão Pública. Reparação do Evento Danoso. Cabimento. Apelação Parcialmente Provida. Pedido Julgado Procedente em Parte. 1. O Apelante Afirma Ter Sofrido Dano Moral, em Razão de Haver Sido Instaurado Inquérito Policial Envolvendo Seu Nome e O Respectivo Cadastro de Pessoas Físicas (Cpf), Quando, na Realidade, O Envolvido Com Os Fatos Delituosos Objeto da Investigação Era Pessoa Com Nome Semelhante Ao Seu. 2. Compulsando Os Autos, É Possível Verificar Que A Certidão de Distribuição Regional (Ações e Execuções), Emitida Pela Justiça Federal da Seção Judiciária do Pará, na Data de 12.05.2009, Registra, em Nome do Apelante, A Existência do Inquérito Policial N. 2008.39.00.000.283-0, em Trâmite, na Época, Junto À 3ª Vara Federal. 3. na Hipótese Está Satisfatoriamente Configurado Erro da Administração, Que Deu Início A Um Procedimento Investigatório Indicando Não Apenas O Nome do Apelante, Mas Também, Dados Pessoais Como O Número do Cpf, Demonstrando Evidente Desídia, Ao Deixar de Adotar As Cautelas Necessárias e Exigíveis, em Tais Casos, Para Que A Pessoa, Cujas Desventuras Sejam Possuir Nome Idêntico Ao do Verdadeiro Investigado, Não Venha A Passar Por Incômodos Semelhantes Aos Experimentados Pelo Autor. 4. O Abalo Experimentado, na Hipótese em Exame, Vai Além do Mero Aborrecimento, Diante do Ônus Que O Estado Acabou Por Impor Ao Apelante, de Comprovar Não Ter Tido Nenhum Envolvimento Com A Conduta Criminosa Objeto da Investigação. 5. na Hipótese, O Montante de R\$ 5.000,00 (Cinco Mil Reais), Diante das Circunstâncias do Caso, Mostra-Se Razoável Para Reparar O Gravame Sofrido, Levando-Se em Conta Que, de Fato, Não Ficou Demonstrada A Alegada Detenção Por 5 (Cinco) Horas na Sede da Polícia Federal, Ônus Que Competia Ao Autor, nos Termos do Art. 373, Inciso I, do Código de Processo Civil (Cpc) de 2015. 6. Juros de Mora Fixados Com Base no Índice de Remuneração da Caderneta de Poupança. 7. A Correção Monetária Deve Ser Levada A Efeito Mediante A Aplicação do Ipca-E, A Partir da Data do Arbitramento. 8. A Incidência dos Juros de Mora, na Espécie, Deve Ser Feita em Consonância Com Os Ditames da Súmula N. 54 do Superior Tribunal de Justiça, A Partir do Evento Danoso. 9. Apelação Parcialmente Provida. Pedido Julgado Procedente, em Parte. nº 00002267220124013701. Relator: Daniel Paes Ribeiro. Brasília, DF, 08 de abril de 2019. **E-DJF**. Brasília, 26 abr. 2019. Disponível em: <<https://arquivo.trf1.jus.br/PesquisaMenuArquivo.asp?p1=00002267220124013701>> Acesso em: 11 maio 2022.

DONEDA, Danilo Cesar Marganhoto. **Da privacidade à proteção de dados pessoais**. 2. ed. São Paulo: Thomson Reuters Brasil, 2020.

DWORKIN, Ronald. **Levando os Direitos a Sério**. São Paulo: Martins Fontes, 2002.

GAGLIANO, Pablo Stolze; PAMPLONA FILHO, Rodolfo. **Novo curso de direito civil, volume 3**. 10. ed. São Paulo: Saraiva, 2012.

_____. **Novo curso de Direito Civil 1: parte geral**. 21. ed. São Paulo: Saraiva Jur, 2019.

GONÇALVES, Carlos Roberto. **Direito Civil Brasileiro, volume 4: Responsabilidade civil**. 7. ed. São Paulo: Saraiva, 2012.

LIMA, Caio César Carvalho. Capítulo II: do tratamento de dados pessoais. In: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. **LGPD: lei geral de proteção de dados comentada**. 2. ed. São Paulo: Thomson Reuters Brasil, 2020. Cap. 2. p. 200-241.

LUGATI, L. N.; ALMEIDA, J. E. de. Da evolução das legislações sobre proteção de dados: a necessidade de reavaliação do papel do consentimento como garantidor da autodeterminação informativa. **Revista de Direito**, [S. l.], v. 12, n. 02, p. 01–33, 2020. Disponível em: <<https://periodicos.ufv.br/revistadir/article/view/10597>>.

MACIEL, Rafael Fernandes. **Manual Prático sobre a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/18)**. Goiânia: Rm Digital Education, 2019.

MEIRELLES, Hely Lopes. **Direito Administrativo brasileiro**. 42. ed. São Paulo: Malheiros, 2016.

MELLO, Celso Antônio Bandeira de. **Curso de Direito Administrativo**. 32. ed. São Paulo: Malheiros, 2015.

MALDONADO, Viviane Nóbrega. Capítulo III: dos direitos do titular. In: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. **LGPD: lei geral de proteção de dados comentada**. 2. ed. São Paulo: Thomson Reuters Brasil, 2020. Cap. 3. p. 241-273.

ONU. Constituição (1948). **Declaração Universal dos Direitos Humanos**. Resolução 217 A III, de 1948. Paris, 10 dez. 1948. Disponível em: <<https://www.unicef.org/brazil/declaracao-universal-dos-direitos-humanos>> Acesso em: 20 abr. 2022.

PINHEIRO, Patrícia Peck. **Proteção de dados pessoais: comentários à lei n. 13.709/2018 (lgpd)**. São Paulo: Saraiva Educação, 2018.

_____. **Proteção de dados pessoais: comentários à lei n. 13.709/2018 (lgpd)**. 3. ed. São Paulo: Saraiva Educação, 2020.

RAMOS, André de Carvalho. **Curso de direitos humanos**. 4. ed. São Paulo: Saraiva, 2017.

RODRIGUES, Laura Secfém; POMPEU, Márcio. **LGPD e decisões automatizadas: onde vamos parar?**. onde vamos parar?. 2021. Disponível em: <<https://www.conjur.com.br/2021-mai-03/opinio-lgpd-decisoes-automatizadas-onde-vamos-parar>>. Acesso em: 14 abr. 2022.

PARANÁ. Tribunal de Justiça do Paraná. APELAÇÃO CÍVEL. AÇÃO DECLARATÓRIA C/C OBRIGAÇÃO DE FAZER E REPARAÇÃO DE DANO MORAL. PRESTAÇÃO DE SERVIÇO DE INTERNET. SENTENÇA QUE JULGOU IMPROCEDENTES OS PEDIDOS COM FUNDAMENTO NO ART. 487 INCISO I DO CÓDIGO DE PROCESSO CIVIL. IRRESIGNAÇÃO DA PARTE AUTORA. CASO EM QUE PARA A CONTRATAÇÃO DE SERVIÇO DE INTERNET FOI CRIADO UM CNPJ EM NOME DA AUTORA COM POSTERIOR BAIXA. FALHA NO DEVER DE INFORMAÇÃO ADEQUADA E CLARA CONFIGURADA. DADOS PESSOAIS UTILIZADOS EM DETRIMENTO À FINALIDADE ESPECÍFICA, EXPLÍCITA E INFORMADA AO SEU TITULAR (ART. 6º, I, LGPD), POIS DESNECESSÁRIO A ABERTURA DE EMPRESA EM NOME DE PESSOA FÍSICA PARA A SIMPLES CONTRATAÇÃO DE SERVIÇOS DE INTERNET. DANO MORAL CONFIGURADO. NECESSIDADE DE REFORMA DA SENTENÇA. RECURSO

CONHECIDO E PROVIDO. Apelação Cível nº 00766189320188160014. Relator: Dartagnan Serpa Sa. Curitiba, 10 de maio de 2021. **Diário de Justiça Eletrônico**. Curitiba, . Disponível em:

<<https://portal.tjpr.jus.br/jurisprudencia/publico/pesquisa.do;jsessionid=a771c81165559dc589f257c352d4?actionType=pesquisar.>> Acesso em: 03 maio 2022.

SÃO PAULO. Tribunal de Justiça. Passagem Forçada – Imóvel Encravado – Encravamento do Imóvel Pertencente Ao Autor Demonstrado Por Laudo Pericial – Passagem Forçada Bem Reconhecida – Exegese do Artigo 1.285 do Código Civil – Indenização Devida Pelo Autor Decorrente do Texto Legal – Ausência de Prova de Que O Encravamento Pode Ser Atribuído À Apelada – Procedência em Parte Mantida – Recurso Não Provido. AC nº 10004527920178260589. Relator: Desembargador Correia Lima. São Paulo, SP, 24 de setembro de 2020. **Diário de Justiça Eletrônico**. São Paulo, 24 set. 2020. Disponível em: <<https://tj-sp.jusbrasil.com.br/jurisprudencia/933887968/apelacao-civel-ac-10004527920178260589-sp-1000452-7920178260589.>> Acesso em: 03 abr. 2022.

SARTORI, Ellen Carina Mattias. Privacidade e dados pessoais: a proteção contratual da personalidade do consumidor na internet. **Revista de Direito Civil Contemporâneo**, São Paulo, v. 9, s.n., p. 49-104, out. 2016. Disponível em: <<http://ojs.direitocivilcontemporaneo.com/index.php/rdcc/article/view/172.>> Acesso em: 22 mar. 2022.

SIMÕES, Bruna. **LGPD e a responsabilidade civil do Estado**. 2021. Disponível em: <<https://www.migalhas.com.br/coluna/migalhas-de-responsabilidade-civil/350717/lgpd-e-a-responsabilidade-civil-do-estado.>> Acesso em: 11 maio 2022.

STF, Portal do. **Ministra suspende MP que prevê compartilhamento de dados com o IBGE por empresas de telecomunicações durante pandemia**. 2020. Disponível em: <<https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=442090&ori=1.>> Acesso em: 18 maio 2022.

TARTUCE, Flávio. **Manual de Direito Civil**: volume único. 5. ed. São Paulo: Método, 2015.

TASSO, Fernando Antonio. Capítulo IV: do tratamento de dados pessoais pelo Poder Público. In: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. **LGPD**: lei geral de proteção de dados comentada. 2. ed. São Paulo: Thomson Reuters Brasil, 2020. Cap. 4. p. 274-325.

VAINZOF, Rony. Capítulo I: disposições preliminares. In: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. **LGPD**: lei geral de proteção de dados comentada. 2. ed. São Paulo: Thomson Reuters Brasil, 2020. Cap. 1. p. 21-199.

VENOSA, Sílvio de Salvo. **Direito Civil**: responsabilidade civil. 13. ed. São Paulo: Atlas, 2013.

XAVIER, Luciana Pedroso; XAVIER, Marília Pedroso; SPALER, Mayara Guibor. Parte II - Diversos tipos de tratamento e questões específicas: capítulo 3 - primeiras impressões sobre o tratamento de dados pessoais nas hipóteses de interesse público e execução de contratos. In: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato. **Lei Geral de proteção de dados pessoais e suas repercussões no Direito Brasileiro**. São Paulo: Thomson Reuters Brasil, 2019. Cap. 3. p. 284-296.

TERMO DE AUTENTICIDADE DO TRABALHO DE CONCLUSÃO DE CURSO

Eu, Pedro César Soares de Macedo Burim
discente regularmente matriculado(a) na disciplina TCC II, da 10ª etapa do curso de Direito, matrícula nº (inserir TIA), período (inserir período), turma (inserir turma), tendo realizado o TCC com o título: Responsabilidade Civil Do Estado Por Danos Causados ao Titular De Dados Pessoais Segundo a LGPD
sob a orientação do(a) Professor(a) Denise Neves Abade
declaro para os devidos fins que tenho pleno conhecimento das regras metodológicas para confecção do Trabalho de Conclusão de Curso (TCC), informando que o realizei sem plágio de obras literárias ou a utilização de qualquer meio irregular.

Declaro ainda que, estou ciente que caso sejam detectadas irregularidades referentes às citações das fontes e/ou desrespeito às normas técnicas próprias relativas aos direitos autorais de obras utilizadas na confecção do trabalho, serão aplicáveis as sanções legais de natureza civil, penal e administrativa, além da reprovação automática, impedindo a conclusão do curso.

São Paulo, 20 de maio de 2022.



Assinatura do discente