REVISTA CONVERSAS CIVILÍSTICAS

ISSN 2763-8448

COMPARTILHAMENTO DE DADOS PESSOAIS SENSÍVEIS ENTRE OS ÓRGÃOS DA ADMINISTRAÇÃO PÚBLICA: UMA ANÁLISE DO DECRETO Nº 10.046/2019 À LUZ DA RELATORIA DA ADPF 695 E ADI 6649/DF

SHARING OF SENSITIVE PERSONAL DATA BETWEEN PUBLIC ADMINISTRATION BODIES: AN ANALYSIS OF DECREE NO. 10,046/2019 IN LIGHT OF THE RAPPORTEURSHIP OF ADPF 695 AND ADI 6649/DF

Carolina Quarantini Leite[1]

Alexandre Barreiros de Carvalho Fonseca[2]

Resumo: Em decorrência da exponencial evolução tecnológica e, consequentemente, maior veiculação de dados pessoais, este artigo científico possui como objetivo dissertar sobre o compartilhamento de dados sensíveis entre órgãos e entidades da Administração Pública mediante análise do Decreto nº 10.046/2019 à luz do julgamento da Arguição de Descumprimento de Preceito Fundamental nº 695 e Ação Direta de Inconstitucionalidade nº 6649/DF. Dessa forma, mediante pesquisa bibliográfica e documental, o presente artigo visa discutir o tratamento de dados pessoais sensíveis e, sobretudo, os limites para seu compartilhamento pelo Poder Público sob égide do princípio da proteção de dados pessoais e necessidade do acesso à informação.

Palavras-chave: Administração Pública; Dados sensíveis; LGPD; Proteção de dados pessoais.

Abstract: As a result of the exponential technological evolution and, consequently, greater dissemination of personal data, this scientific article aims to discuss the sharing of sensitive data between bodies and entities of the Public Administration through the analysis of Decree nº. 10,046/2019 considering the judgment of the Allegation of Non-Compliance with Fundamental Precept nº 695 and Direct Action of Unconstitutionality nº 6649/DF. Thus, through bibliographic and documentary research, this article aims to discuss the processing of sensitive data and, above all, the limits to its sharing by the Government under the aegis of the principle of personal data protection and the need for access to information.

Keywords: Public administration; Sensitive data; Access to Information Law; LGPD; Protection of personal data.

[1] Graduada em Direito pela Universidade Católica do Salvador (UCSAL). E-mail: carolinaquarantini@hotmail.com

[2] Doutorando em Políticas Sociais e Cidadania pela Universidade Católica do Salvador (UCSAL), Mestre em Filosofia (UFBA), Pós-graduado em Direito Público pela Faculdade Baiana de Direito; Graduado em Direito (UCSAL) e Filosofia (UFBA). Docente da Universidade Católica do Salvador (UCSAL). E-mail: alexandre.fonseca@pro.ucsal.br

ISSN 2763-8448

1. INTRODUÇÃO

Este artigo científico possui como objeto a análise do Decreto nº 10.046/2019 que dispõe sobre o compartilhamento de dados na administração pública federal, institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados. Enfatiza-se que esta análise será realizada à luz do voto da relatoria da Ação de Arguição de Descumprimento de Preceito Fundamental (ADPF) 695 e Ação Direta de Inconstitucionalidade (ADI) 6649/DF.

É possível o compartilhamento de dados sensíveis no ordenamento jurídico brasileiro? Seria possível transpor esses dados para benefício da Administração Pública em detrimento do princípio fundamental da privacidade? Quais os limites impostos para cercear o compartilhamento irrestrito? Essas são algumas das indagações que cercam o presente debate.

No Brasil, o compartilhamento de dados pessoais entre órgãos da administração pública federal constitui-se um tema recente e, consoante dizeres de Cesar Alvarez (2020) em artigo do programa ObservaBR, Caminhos da Reconstrução e Transformação do Brasil da Fundação Perseu Abramo, os dados pessoais são considerados o “novo petróleo brasileiro”. Portanto, visando a proteção dos cidadãos, é necessário discutir os limites do compartilhamento de dados pessoais, sobretudo, aqueles sensíveis à garantia da inviolabilidade da intimidade, imagem e vida privada, bem como a razoabilidade de determinados decretos do Poder Executivo.

Com a instituição da Lei Geral de Proteção de Dados (LGPD), a proteção de dados pessoais configura-se como garantia da inviolabilidade da intimidade, imagem e vida privada. Entretanto, o Decreto nº 10.046/2019 tenta viabilizar o compartilhamento de dados considerados sensíveis à LGPD e, diante dessa problemática, o Supremo Tribunal Federal, através do julgamento da ADPF 695 e ADI 6649/DF, discute a constitucionalidade de determinados dispositivos do mencionado decreto. Portanto, pergunta-se: quais os limites do compartilhamento de dados sensíveis entre os órgãos da Administração Pública a partir da Lei Geral de Proteção de Dados (LGPD)?

ISSN 2763-8448

Objetiva-se de forma geral apresentar discussão argumentativa acerca do Decreto nº 10.046/2019, desenvolvendo o seu processo de formulação, bem como analisar o voto da relatoria da ADPF 695 e ADI 6649/DF.

Por fim, a pesquisa possui finalidade exploratória e explicativa, mediante análise de bibliografia especializada e documentação jurídica, utilizando o método hipotético deduzido. As bibliotecas digitais acessadas foram: Biblioteca digital da Universidade Católica do Salvador e Portal Periódicos Capes (Coordenação de Aperfeiçoamento de Pessoal de Ensino Superior), com a utilização dos seguintes descritores de busca: proteção de dados pessoais, dados sensíveis, LGPD.

2. BREVE PANORAMA HISTÓRICO DA LEI DE PROTEÇÃO DE DADOS NO BRASIL

As primeiras cautelas adotadas para a governança dos dados pessoais surgiram na medida em que o processo de globalização demandou um maior fluxo das bases de dados, principalmente, pessoais na economia digital, impulsionada pela globalização (Pinheiro, 2023).

Com a apreensão acerca do destino e utilização dos dados e o avanço exponencial da tecnologia, necessitou-se reafirmar o compromisso entre as instituições e indivíduos quanto a proteção e garantia dos direitos humanos fundamentais presentes na Declaração Universal dos Direitos Humanos (DUDH) de 1948, sobretudo, o direito à privacidade (Pinheiro, 2023).

A primeira legislação específica sobre a proteção de dados, ainda que não fosse destinada para o âmbito virtual, *Hessisches Datenschutzgesetz* (*The Hesse Data Protection Act*), data de 1970 no estado de Hessen, na Alemanha. No entanto, o entendimento da proteção de dados pessoais como um direito humano e fundamental no ordenamento jurídico-constitucional é fruto de um longo processo (Sarlet, 2021b).

A partir da reafirmação do compromisso entre indivíduos e instituições, iniciou-se a discussão acerca da temática na União Europeia (UE), especificamente através do partido *The Greens*, culminando na promulgação da *General Data Protection Regulation* (GDPR) em 27 de abril de 2016. A partir da supramencionada legislação, a União Europeia começou a exigir que os países com quem tinha relações comerciais

ISSN 2763-8448

também elaborassem uma legislação semelhante, sob pena de dificultar as negociações comerciais ou, até mesmo, rompê-las (Pinheiro, 2023).

No Brasil, a primeira menção aos dados pessoais ocorreu no Projeto de Lei 2.796 de 1980, proposto pela ex-deputada Cristina Tavares, dispondo que "assegura aos cidadãos acesso às suas informações constantes de bancos de dados e dá outras providências". Esse projeto, no entanto, foi arquivado (DONEDA *et al*, 2021).

Lugati e Almeida (2022) dissertam que o tratamento dos dados é abordado desde 1988 através da Carta Magna, podendo ser observado por meio do direito da personalidade, liberdade de expressão, direito à informação, inviolabilidade da vida privada e intimidade, *habeas data* e interceptação das comunicações telefônicas, telegráficas ou de dados.

Contudo, anteriormente à 1988, já existiam legislações que regulamentavam o acesso e retificação de dados pessoais em São Paulo (Lei Estadual nº 5.702, de 5 de junho de 1987) e Rio de Janeiro (Lei Estadual nº 824, de 28 de dezembro de 1984). Esses dispositivos foram cruciais para a fomentação da questão do *habeas data* na Constituição Brasileira de 1988 (DONEDA *et al*, 2021).

Em termos de legislações infraconstitucionais, a temática era abordada de forma indireta e muito sucintamente no Código de Defesa do Consumidor (CDC), na Lei do Cadastro Positivo (Lei nº 12.414/2011) e no Marco Civil da Internet.

O Código de Defesa do Consumidor de 1990, em seu art. 43, atribui, ainda que incipiente e mais direcionada ao direito à comunicação, uma certa proteção ao titular de dados, ao mencionar no seu parágrafo segundo que "a abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele" (LUGATI e ALMEIDA, 2022).

A Lei do Cadastro Positivo (Lei nº 12.414/2011), por sua vez, é considerada como uma lei vanguardista já que, diferentemente do CDC, aborda o consentimento como base para efetivação da proteção (LUGATI e ALMEIDA, 2022).

A mencionada legislação, consoante *caput* do art. 1º, atua nos bancos de dados que detêm informações sobre as relações de adimplemento de crédito de pessoas naturais e jurídicas. Ademais, a proteção ao titular pode ser observada quando há disposição sobre os direitos do cadastrado (art. 5º), sobretudo, quando há menção no inciso VII sobre: "ter os seus dados pessoais utilizados somente de acordo com a finalidade para a qual eles foram coletados" (Brasil, 2011).

ISSN 2763-8448

O Marco Civil da Internet advém após um caso de espionagem envolvendo o Brasil na Agência Nacional de Segurança dos Estados Unidos, sendo aprovado no evento NetMundial durante o mandato da ex-presidente Dilma Rousseff, e, apesar de mencionar o consentimento, também não tratou especificamente sobre a proteção de dados (Lugati e Almeida, 2022).

Somente em 2010, uma legislação brasileira específica, fruto de um debate do Mercosul em 2005, para a regulamentação da proteção de dados começou a ser projetada - a Lei Lei Geral de Proteção de Dados – atribuindo importância fundamental e precisa ao instituto do consentimento do titular, tendo sido promulgada em 2018 (Lugati e Almeida, 2022).

Sendo exposto pelo Ministério da Justiça em 30 de novembro de 2010, o primeiro anteprojeto do que hoje é a LGPD foi elaborado pela Secretaria Nacional do Consumidor (Senacon) e, posteriormente, objeto de um debate público virtual – ainda parcialmente disponível -organizado juntamente com a Fundação Getúlio Vargas, Observatório da Internet e Comitê Gestor da Internet do Brasil (Doneda *et al*, 2021).

No período compreendido entre 2011 e 2015, o texto-base do anteprojeto foi modificado por diversas vezes, sendo que essas modificações ocorreram em duas principais fases. A primeira fase corresponde ao trâmite interno no governo federal e a segunda consiste em uma etapa externa, envolvendo a população, grandes juristas e outros *experts* na temática (Doneda *et al*, 2021).

Em 2016, o texto foi encaminhado ao Congresso Nacional, sendo protocolada como PL 5.276/2016 na Câmara dos Deputados e dispondo sobre “o tratamento de dados pessoais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural" (Doneda *et al*, 2021).

3. CONCEITOS ACERCA DOS DADOS PESSOAIS SENSÍVEIS NA DOUTRINA BRASILEIRA E A LEI GERAL DE PROTEÇÃO DE DADOS (LGPD).

Consoante dispõe o art. 5º, I, da LGPD, entende-se por dados pessoais o conjunto de informações relacionadas à pessoa natural identificada ou identificável –

ISSN 2763-8448

esta potencialmente pode ter sua identidade revelada e aquela, de fato, apresenta-se por livre consentimento (Brasil, 2018).

Acrescenta-se ainda que os dados pessoais não englobam tão somente o nome, sobrenome, idade, endereço residencial ou eletrônico de um indivíduo. Pode-se incluir nesse gênero: informações sobre localização, placas de automóveis, histórico de compras, número do *Internet Protocol* (IP), dados acadêmicos e outros inerentes à pessoa natural viva (Pinheiro, 2023).

Acerca dos dados pessoais sensíveis, Gonçalves e Varella (2018) apontam que não há uma uniformização no conceito da expressão, configurando-se em uma situação de insegurança ao deixar lacunas para interpretações diversas. Assim, exemplifica-se a adoção de termos distintos: dados restritos, informações protegidas e dados sigilosos por, respectivamente, IBGE (2003), INEP (2014) e IPEA (2014).

O inciso II da LGPD considera que os dados pessoais sensíveis consistem nas características da personalidade da pessoa natural, a título de exemplo: origem racial ou étnica, religiosidade, posição política, saúde ou vida sexual, genética ou biométrica e outras (Brasil, 2018).

A Lei nº 12.527/2011, por sua vez, prevê em seu art. 4º, III, a informação sigilosa, esta consiste em uma categoria com acesso público restrito temporariamente em face da sua importância para segurança da sociedade e do Estado (Brasil, 2011)

Em síntese, Sarlet e Ruaro (2021a, p. 6) asseveram ainda que “[...] os dados sensíveis são, em vista disto, nucleares para a prefiguração e para a personificação do sujeito de direito no contexto atual”.

O dado sensível, portanto, é caracterizado a partir da utilização de forma discriminatória, sendo possível mensurar a afetação direta à pessoa humana (Sarlet e Ruaro, 2021a).

A utilização do termo sensível, logicamente, não é sem fundamento uma vez que significa um perigo iminente em casos de divulgação. Trata-se de uma espécie de dados que, sendo disposto irrestritamente, produziria danos irreparáveis.

Sob esse viés, o enfoque de uma maior proteção aos dados sensíveis é justificado através da probabilidade que a sua má utilização pode gerar danos gravíssimos (Gonçalves e Varella, 2018)

ISSN 2763-8448

Ressalta-se que o instituto do consentimento não é o único requisito autorizador para o tratamento de dados, mas, sim, uma das diversas hipóteses, dentre eles, cabe ainda citar o legítimo interesse. Esse requisito é pautado em uma fundamentação considerada legítima e respaldada na finalidade, necessidade e proporcionalidade na utilização dos dados. O destinatário, obrigatoriamente, deve especificar as suas motivações, intenções com o tratamento e meios a alcançá-lo. Nessa hipótese não há tolerância para uma fundamentação vaga e genérica, é necessária precisão nas informações prestadas (Doneda *et al*, 2021).

Outras hipóteses são mencionadas pelo art. 7º da Lei Geral de Proteção de Dados, tais como: realização de pesquisas, cumprimento de obrigação legal, exercício regular de direitos em processo judicial, proteção do crédito, etc (Brasil, 2018).

Especificamente sobre os dados sensíveis, o legítimo interesse não é aplicável a seu tratamento, devendo incidir as demais hipóteses elencadas pelo art. 11 da LGPD (Brasil, 2018).

A hipótese prevalente, teoricamente, deveria ser o consentimento do titular, todavia, a doutrina critica severamente a técnica legislativa adotada no art.11 a respeito de que deveria haver uma posição de igualdade entre as hipóteses elencadas (Doneda *et al*, 2021).

O consentir do titular divide-se em específico e destacado. Esse é a manifestação expressa sobre todos as finalidades detalhadas pelo destinatário enquanto aquele refere-se ao acesso do titular ao documento que evidencia e destaca os fatos do tratamento, aqui, a vontade deve ser expressa em destaque no documento que assente o tratamento de seus dados (Doneda *et al*, 2021).

4. O DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS PESSOAIS E O ACESSO À INFORMAÇÃO

Leciona Sarlet (2021b) que o direito à proteção de dados pessoais configura-se como um direito fundamental assegurado na Carta Magna brasileira. Todavia, ressalta-se que não há expressamente na Constituição Federal de 1988 essa proteção, mas, sim, fundamentos implícitos.

ISSN 2763-8448

Assim, o art. 5º, § 2º, do texto constitucional dispõe que os direitos e garantias expressamente elencados na Constituição não excluem outros advindos do regime ou princípios adotados e tratados internacionais nos quais o Brasil atua como membros. Trata-se, portanto, do reconhecimento da dinamicidade da sociedade civil e uma tentativa do ordenamento jurídico acompanhar as mudanças e evoluções.

Em julgamento histórico do Supremo Tribunal Federal (STF) diante a medida cautelar na Ação Direta de Inconstitucionalidade (ADI) 6.387/DF (e nas ADIs 6.388, 6389, 6.390 e 6.393) em face da Medida Provisória (MP) 954/2020 – que regulamentava o compartilhamento de dados de telefonia fixa e móvel de milhões de brasileiros ao Instituto Brasileiro de Geografia e Estatística (IBGE), a relatora e ex-ministra Rosa Weber reconheceu o direito à proteção de dados pessoais como um direito fundamental independente do direito à privacidade e à autodeterminação informativa pela Suprema Corte.

Nesse sentido, Sarlet (2021b) alerta que não se deve confundir o direito à proteção de dados com o direito à privacidade uma vez que se tratam de direitos autônomos e com objetos tutelados diferentes.

A Constituição Federal de 1988 dispõe em seu art. 5º, inciso X, que a intimidade, a vida privada, honra e a imagem das pessoas são preceitos invioláveis, sendo, em hipótese de violação, assegurado o direito à reparação por danos morais ou materiais (Brasil,1988).

Diante da consagração do direito à privacidade, percebe-se que a Constituição Federal de 1988 adota o sentido amplo do termo privacidade, justamente, para contemplar diversas manifestações da esfera íntima, privada e personalidade das pessoas (Cunha Júnior, 2018).

Cunha Júnior (2018, p. 634) leciona ainda que a privacidade, basicamente, consiste na faculdade do indivíduo de impedir a intromissão de terceiros na sua vida particular, bem como o acesso e publicação de informações atinentes à sua privacidade e intimidade.

Ademais, o direito à privacidade abrange, devido a conexão, o direito à intimidade; à vida privada; e ao sigilo das correspondências e das comunicações telegráficas, de dados e das comunicações telefônicas (Cunha Júnior, 2018).

Entende-se por direito à intimidade aquele associado à intimidade do indivíduo, afastando-o da publicidade. Refere-se ainda a proteção dos seus segredos, vida

ISSN 2763-8448

sexual e convicções. Por outro lado, o direito à vida privada consiste em uma reserva da vida com outros indivíduos, familiares, amigos ou colegas de trabalho (Cunha Júnior, 2018)

Quanto ao direito ao sigilo de correspondências e das comunicações telegráficas, de dados e das comunicações telefônicas, Ferraz Júnior (1993) infere que se trata da inviolabilidade do sigilo voltado à comunicação dos objetos. Refere-se aqui a invasão de um terceiro, que não possui qualquer vínculo ou relação, em uma transmissão privativa.

Ferraz Júnior (1993) firma o entendimento do Supremo Tribunal Federal no sentido de que a terminologia "dados" do art. 5º, XII, da CF/88 refere-se à comunicação dos dados e não de forma direta aos dados propriamente ditos.

Portanto, percebe-se que a proteção à privacidade vincula-se a assegurar a personalidade, o cerne da tutela dos dados pessoais consiste em proteger de forma mais ampla toda informação de uma pessoa natural independentemente da esfera de sua vida em que o dado esteja localizado (Sarlet, 2021b).

Por todo o exposto, em 10 de fevereiro de 2022, as mesas da Câmara dos Deputados e do Senado Federal, promulgam a Emenda Constitucional nº 115 em observância à autonomia do direito à proteção de dados pessoais. Acrescenta-se ao *caput* do art. 5º da CF/88, o inciso LXXIX, responsável por assegurar a proteção dos dados, incluindo no âmbito digital (Brasil, 2022).

O *caput* do art. 21 do texto constitucional, agora, inclui o inciso XXVI, dispondo como competência material da União "organizar e fiscalizar a proteção e o tratamento de dados pessoais, nos termos da lei" (Brasil, 2022).

Ao art. 22 da CF/88, que disserta a competência privativa da União para legislar, inclui-se o inciso XXX, mencionando a proteção e tratamento de dados pessoais (Brasil, 2022).

A autodeterminação informativa, por sua vez, ultrapassa o poder de decisão do titular sobre suas informações. Flôres e Silva (2023) elucidam que representa uma garantia de que o titular possa dispor como bem entender sobre seus dados, bem como proporciona o exercício democrático.

Ademais, apesar da existência de uma legislação infraconstitucional específica, a segurança do indivíduo no espaço digital necessita de uma maior assistência, uma

ISSN 2763-8448

vez que o ambiente virtual ou digital, conforme lecionam Sarlet e Ruaro (2021a), é caracterizado pela volatilidade, incerteza, complexidade e ambiguidade.

Dessa forma, mediante um cenário em que há evolução tecnológica, a exponencial circulação de informações e, sobretudo, o valor político e econômico que os dados pessoais possuem para a construção de novas formas de controle (algoritmos, inteligência artificial e *Big Data*), aumenta drasticamente a vulnerabilidade de um indivíduo, tornando a inviolabilidade de seu direito à privacidade um verdadeiro desafio. Na Lei Geral de Proteção de Dados (LGPD), o tratamento dos dados pessoais, desde o gerenciamento até o compartilhamento, deve ser obrigatoriamente realizado de forma segura, sob pena de responsabilização e multas que podem chegar a 50 milhões de reais (Sarlet e Ruaro, 2021a).

De mais a mais, justamente por conta de sua natureza, a proteção de dados pessoais consiste em um princípio que está intrinsecamente ligado à dignidade da pessoa humana.

Entende-se por dignidade da pessoa humana a qualidade intrínseca, não renunciável e inalienável que atribui a qualidade de humano a um indivíduo, isto é, trata-se da própria condição humana. Essa condição inerente, portanto, deve ser respeitada e salvaguardada (Sarlet, 2007).

Logo, sendo os dados pessoais características e informações referentes à identidade de um indivíduo, quando há a exposição sem o correto tratamento e seu consentimento e, assim, culminando no vazamento de seus dados e geração de danos irreparáveis, evidencia-se aqui uma violação à sua dignidade.

Consoante art. 5º, XXXIII, da Constituição Federal de 1988, todos possuem direito de receber informações de seu interesse particular, coletivo ou geral através dos órgãos da Administração Pública no prazo definido por lei, salvo informações sigilosas.

Sob essa ótica, a Lei 12.527 de 18 de novembro de 2011 (Lei de Acesso à Informação) objetiva a transparência e publicidade de informações, desde que nos limites da legislação, reafirmando e consolidando um regime democrático.

Destarte, sobre a informação infere-se que é primordial para as sociedades democráticas e constitui como um direito, inclusive, em relação ao âmbito público diante o qual deve haver consonância com os princípios da moralidade e publicidade. Nesse *mister,* a transparência, ao mesmo tempo em que funciona como uma espécie

ISSN 2763-8448

de controle social, possibilita que a Administração Pública crie e execute políticas públicas (Flôres e Silva, 2023).

Assim como ocorre com os demais direitos fundamentais, a proteção de dados pessoais está submetida a limites - os quais configuram-se como "condição prévia de legitimação constitucional das restrições" - com a finalidade de igualmente proteger outros direitos ou bens jurídicos, obviamente, seguindo os critérios de proporcionalidade. Nessa esfera, é de extrema importância a distinção entre os dados pessoais sensíveis àqueles que são alheios à espécie (Sarlet, 2021b).

Sarlet (2021b) exemplifica os limites por meio do julgamento da Suspensão de Segurança nº 3.902, ocorrido em 24 de abril de 2015 e de relatoria do ex-ministro Teori Zavascki, em que se discutia o entrave entre o acesso a informações e o direito à proteção de dados pessoais sensíveis dos servidores públicos. O acesso à informação, juntamente, com os princípios da publicidade e da transparência, contribuiu para que o Supremo Tribunal Federal (STF) considerasse que a proteção da privacidade dos servidores é menor do que a de um cidadão comum, logo, sendo constitucional a divulgação dos seus vencimentos e benefícios.

Nessa senda, ao tempo em que a LGPD assegura a proteção de dados, a Lei nº 12.527 de 2011 possui como objeto a ser tutelado o acesso à informação. Nota-se aqui a "colisão autêntica de direitos fundamentais", expressão denominada por José Joaquim Canotilho, na qual o exercício do direito de um indivíduo vai de encontro ao exercício do direito de outrem (Aragão, 2011).

Diante desse impasse, Robert Alexy reconhece que não há um princípio absoluto e, portanto, propõe o sopesamento desses -aqui, analogamente, os direitos fundamentais em colisão. Nessa teoria, prevalece o princípio que melhor enquadra-se nas especificidades do caso concreto, logo, trata-se de um meio de coexistência de princípios sem a anulação daquele que possui menor peso (Aragão, 2011).

Ainda que haja a prevalência, por exemplo, do direito à informação, os entes públicos autorizados devem obrigatoriamente dispor de uma gestão transparente e proteger as informações, sobretudo, sigilosas e pessoais (Brasil, 2011).

Consoante art. 23 da LGPD, quanto ao tratamento dos dados, as pessoas de direito público devem obrigatoriamente executá-lo em conformidade com sua finalidade e interesse público. Entende-se por interesse público a atuação do Estado

ISSN 2763-8448

em consonância com os interesses da sociedade, objetivando o alcance do maior número de indivíduos (Souza; Barrancos; Maia, 2019).

5. SIMILARIDADES E PRINCIPAIS MUDANÇAS ENTRE O DECRETO Nº 10.046/2019 E O DECRETO Nº 8.789/2016

Publicado em 10 de outubro de 2019, o Decreto nº 10.046 – editado pelo ex-Presidente da República, Jair Messias Bolsonaro – dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e do Comitê Central de Governança de Dados. Trata-se de um diploma legislativo que é posterior ao Decreto nº 8.789 de 2016, este editado pelo ex-Presidente da República, Michel Temer.

Os dados cadastrais, no decreto de 2016, embarcavam os identificadores cadastrais inerentes à pessoa natural e jurídica, tais como Cadastro Nacional de Pessoas Físicas (CPF), Cadastro Nacional de Pessoas Jurídicas (CNPJ), razão social, nome civil ou social, data de nascimento, vínculo empregatício e tantas outras informações (Brasil, 2016).

Todavia, no decreto de 2019, esses dados cadastrais adquirem uma nova perspectiva, incluindo os atributos biográficos, biométricos e genéticos. Consoante o art. 2º, entende-se por atributos biográficos os dados da pessoa natural advindos dos fatos de sua vida - apesar do termo vago, o decreto exemplifica “fatos de sua vida” como nome, data de nascimento, filiação, sexo, endereço e outros -; os atributos biométricos, por sua vez, consistem nas características biológicas e comportamentais que podem ser coletadas para o reconhecimento da pessoa natural – a título de exemplo: digitais dos dedos, retina, íris dos olhos, formato da face, voz, maneira de andar e etc. -; por fim, os atributos genéticos são relativos as características herdadas dos entes ascendentes e obtidas por análise científica (Brasil, 2019).

Enquanto o Decreto 8.789/2019, permitia o compartilhamento automático desses dados, a lei vigente amplia as formas de intercomunicação entre bases e plataformas, instituindo o Cadastro Base do Cidadão (*vide* art. 16). Nessa base, será possível o cruzamento de informações provenientes da execução de políticas públicas que contenham exclusivamente dados biográficos e biométricos, logo, excluindo os

ISSN 2763-8448

dados genéticos (art. 18, §6º). Percebe-se que esse dispositivo permite o compartilhamento para além dos dados cadastrais, abrangendo os dados pessoais e, inclusive, os dados sensíveis (Brasil, 2019)

Quanto ao cruzamento de informações entre bases diversas, o Decreto nº 11.266 de 2022, dispositivo responsável por alterar, veda o tratamento que vise mapear ou explorar comportamentos individuais ou coletivos de cidadãos sem o devido consentimento e transparência da motivação e finalidade (Brasil, 2022).

O diploma legislativo anterior ao vigente, restringia-se aos órgãos e entidades da administração pública federal direta e indireta e regulamentava a intercomunicação de dados em dois níveis, sendo o primeiro, preferencialmente, de forma automática - disposição temerária - e o segundo conforme a necessidade dos órgãos interessados quanto aos dados não cadastrais e individualizados. Ademais o acesso a base de dados poderia ser realizado somente mediante solicitação ao órgão responsável com a identificação do interessado, a descrição precisa dos dados requeridos e a finalidade do uso (Brasil, 2016).

Não obstante, a transmissão dos dados autorizados a outros órgãos e entidades era vetada pelo art. 9º, salvo concessão expressa do responsável pela base de dados (Brasil, 2016).

Por outro lado, o Decreto nº 10.046/2019 expande a governança do compartilhamento de dados para os poderes legislativo e judiciário, acrescentando-se como fim a operação mais eficaz no tratamento dos dados e estabelecendo três níveis de compartilhamento: amplo, restrito e específico. O compartilhamento amplo refere-se aos dados públicos que são dispostos a população sem qualquer tipo de restrição, justamente, para salvaguardar o princípio da transparência; o restrito, por sua vez, permite o compartilhamento dos dados sob sigilo às entidades e órgãos elencados pelo art. 1º para a concretização de políticas públicas; e, por fim, o compartilhamento específico atribui acesso aos dados sob sigilo à determinados órgãos e entidades (Brasil, 2019).

A classificação do compartilhamento (amplo, restrito e específico), no entanto, compete ao Comitê Central de Governança de Dados consoante I do art. 21. Esse Comitê, antes das alterações de 2022 e 2023, era composto tão somente por representantes da administração pública federal - logo, sem qualquer representação da Câmara dos Deputados e Senado Federal - e responsável pelos ditames sobre a

ISSN 2763-8448

gestão do Cadastro Base do Cidadão, dos níveis de compartilhamento e, inclusive, com poderes (Brasil, 2019).

6. DIVERGÊNCIAS ENTRE O DECRETO Nº 10.046/2019 E A LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

A Lei nº 13.709/2018 (LGPD) é considerada um marco fundamental para a proteção de dados pessoais no Brasil uma vez que aborda precisa e estritamente a temática, diferentemente, do período anterior à sua instituição, que a tratava de forma muito sucinta, genérica e esparsa. Logo, trata-se de uma legislação que, desde seu projeto de lei, foi formulada para atuar como uma referência no ordenamento jurídico já que houve contribuição da população brasileira e *experts* e, sobretudo, observância aos ditames constitucionais.

O art. 6º da LGPD elenca dez princípios, sendo eles: finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização e prestação de contas. Esses princípios, juntamente, com a boa-fé devem basear o tratamento de dados pessoais (Brasil, 2018).

Contudo, na compulsão do texto do Decreto nº 10.046/2019, verifica-se que, antes das alterações efetuadas por decretos subsequentes – Decretos nº 10.332/2020, 11.266/2022 e 11.524/2023 -, não havia menção dos dados pessoais e dados sensíveis, mas tão somente termos alheios à LGPD, tais como: atributos biográficos, biométricos e genéticos.

Enfatiza-se ainda que, durante toda a redação do dispositivo, novamente, antes das alterações, a LGPD é citada por três vezes. A primeira citação é referente ao compartilhamento amplo das informações que deverão observar o disposto na legislação de proteção de dados; a segunda aborda sobre a coleta, o tratamento e o compartilhamento dos dados que deverão seguir os padrões do art. 23 da LGPD; e, por fim, as dispensas para efetivação do compartilhamento mediante as diretrizes do art. 3º da legislação referência (Brasil, 2019).

A Lei Geral de Proteção de Dados possui um capítulo, IV, direcionado exclusivamente para o tratamento de dados pessoais pelo público, dissertando sobre

ISSN 2763-8448

diretrizes a serem seguidas, competência dos órgãos e entidades públicas, a vinculação entre compartilhamento e a finalidade com a execução de políticas públicas e tantos outros preceitos (Brasil, 2018).

Observa-se que o art. 26 da LGPD prevê que o compartilhamento dos dados pessoais deve seguir os princípios elencados pelo art. 6º, quais sejam: finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização (Brasil, 2018).

No entanto, ao mencionar expressões, como “compartilhamento amplo” e “fatos da vida”, sem a devida precisão, o Decreto de 2019 evidencia uma colisão, justamente, ao não especificar o tratamento ao qual os dados coletados devem submeter-se.

Quanto a instituição do Comitê Central de Governança de Dados, percebe-se que o decreto, em seu art. 22, restringe a atuação do comitê à membros pertencentes exclusivamente da Administração Pública Federal, excluindo a participação da sociedade civil e de *experts* da temática, assim, violando os princípios do regime democrático. Diante disso, as alterações pós promulgação do ato administrativo visam justamente a sua adequação, abrangendo sua a representação.

7. A ARGUIÇÃO DE DESCUMPRIMENTO DE PRECEITO FUNDAMENTAL (ADPF) 695 E A AÇÃO DIRETA DE INCONSTITUCIONALIDADE (ADI) 6.649

Ajuizada pelo Partido Socialista Brasileiro (PSB) e com petição protocolada em 16 de junho de 2020, a arguição de descumprimento de preceito fundamental remete à análise da Suprema Corte o compartilhamento indiscriminado e massivo de dados pessoais relacionados aos registros de carteiras de habilitação, tais como: nome, filiação, endereços, telefones, dados dos veículos e fotos dos portadores da Carteira Nacional de Habilitação (CNH) pelo Serviço Federal de Processamento de Dados (SERPRO) à Agência Brasileira de Inteligência (ABIN) com fulcro no Decreto nº 10.046/2019.

De acordo com a exordial do Requerente, o tratamento da ABIN, responsável por planejar, executar, coordenar, supervisionar e controlar as atividades de

ISSN 2763-8448

inteligência do país, era periclitante para a dignidade da pessoa humana, intimidade, privacidade, autodeterminação informativa e proteção de dados uma vez que ia de encontro aos princípios da publicidade e transparência por não haver precisão e clareza na finalidade e sem qualquer razoabilidade e proporcionalidade na execução do ato. Ademais, questiona-se o compartilhamento de dados pessoais, inclusive, sensíveis, de milhões de brasileiros entre SERPRO à ABIN para fins de inteligência estatal, que não possui respaldo legal no ordenamento jurídico.

Em sede de medida cautelar, atendendo ao requisito do *fumus boni iuris* ao demonstrar a flagrante violação aos princípios constitucionais, bem como ao *periculum in mora*, requereu a concessão desta para impedir ou cessar imediatamente o compartilhamento dos dados entre SERPRO à ABIN, assim, para que sejam inutilizados.

Por fim, pugnou pela procedência da ADPF, confirmando a medida cautelar, afastando o compartilhamento de dados da forma mencionada pela arguição, devendo ser realizada a devida aplicação e proteção aos ditames constitucionais. Subsidiariamente, solicita a conversão da ADPF para ADI caso seja entendimento da Suprema Corte, possibilitando a interpretação dos seguintes dispositivos do supramencionado decreto em harmonia à Carta Magna: o art. 1º, atribuindo a este qualidade de rol taxativo e exaustivo e, consequentemente, afastando a hipótese de finalidade em prol da atividade de inteligência; e art. 3º, garantindo a sujeição do compartilhamento pela administração pública às diretrizes da LGPD.

Por outro lado, ajuizada pelo Conselho Federal da Ordem dos Advogados do Brasil (CFOAB) e protocolada em 23 de dezembro de 2020, a ação direta de inconstitucionalidade com pedido cautelar foi proposta em face de determinados dispositivos do Decreto 10.046/2019, declarando inconstitucionalidade formal e material, que extrapola os poderes conferidos ao Presidente da República e viola os direitos fundamentais à dignidade da pessoa humana, intimidade, privacidade, sigilo dos dados, proteção de dados pessoais e autodeterminação informativa.

Preliminarmente, o Conselho requereu a distribuição por dependência da exordial à ADPF nº 695/DF, consoante art. 69 do Regime Interno do Supremo Tribunal Federal, uma vez que a causa de pedir de ambas as ações possuem conexão, justamente, por abordarem sobre a proteção de dados pessoais, o compartilhamento de dados pela Administração Pública e a constitucionalidade do Decreto de 2019. No

ISSN 2763-8448

mérito, sustenta a inconstitucionalidade formal do dispositivo já que o decreto adentraria em matérias privativas de leis, conferindo poderes além dos já previstos ao Presidente da República e, assim desrespeitando o art. 84, incisos IV e VI, alínea 'a'; quanto à inconstitucionalidade material, pode-se vislumbrar na violação aos direitos fundamentais já mencionados.

O maior questionamento da ADI volta-se ao advento de uma ferramenta de vigilância estatal pois, além da inclusão de dados pessoais considerados como básicos, o decreto, apesar de não mencionar expressamente a o termo "dados pessoais sensíveis", incluí o compartilhamento de atributos biométricos, definidos como características biológicas e comportamentais da pessoa natural, sendo elas: digitais dos dedos, íris dos olhos, formato da face, voz, maneira de andar e retina.

Na qualidade de *amicus curiae,* o Laboratório de Políticas Públicas e Internet (LAPIN) consiste em um centro de pesquisa fundado na Universidade de Brasília (UnB) em 2016. A atuação do laboratório está circunscrita na investigação e análise da tríade: direito, tecnologia e sociedade. Consiste em uma entidade que possui influência na prestação de informações aos detentores de poder decisório nos temas de proteção de dados, privacidade, direitos humanos e outros.

A entidade cientificou ao órgão de cúpula do Poder Judiciário que o Comitê Central de Governança de Dados recomendou a submissão dos dados pessoais ao nível de compartilhamento restrito. A cartilha elaborada pelo Comitê contém dados considerados sigilosos, sensíveis, que estariam à disposição e com acesso pleno a todos os órgãos e entidades do Estado, violando os fundamentos basilares da LGPD, sobretudo, quanto à proteção de dados pessoais.

Em sede de análise da ADI 6.649, a Advocacia-Geral da União (AGU), preliminarmente, requereu a inadmissão da ação, vez que a exordial fundamentou a inconstitucionalidade do Decreto em face de normas infraconstitucionais e, não, da Constituição. De acordo com a manifestação da AGU, "a indagação relativa à adequação a dispositivos infraconstitucionais é alheia ao âmbito cognitivo dos processos de controle concentrado de constitucionalidade"

Apesar de concepções diversas, ambas ações convergem para uma matéria: o tratamento de dados pessoais pela Administração Pública. Logo, o relator, Min. Gilmar Mendes, proferiu voto conjunto à ADI 6.649 e ADPF 695.

ISSN 2763-8448

Inicialmente, diante da ADPF 695, nota-se que há, consoante dizeres do próprio ministro relator, uma "tentativa obscura de compartilhamento de dados pessoais com órgãos pertencentes ao Sistema Brasileiro de Inteligência". Nesse sentido, relembra-se o julgamento da ex-ministra Rosa Weber acerca da MP 957/2020, anteriormente já mencionada, declarando a inconstitucionalidade da medida em virtude da periculosidade que ela representava para o regime democrático.

Destarte, para evitar a retirada total do texto impugnado do ordenamento jurídico, utilizou-se a técnica da interpretação para adequar o referido dispositivo à Constituição. A declaração da inconstitucionalidade, removendo por completo o decreto, seria danosa e periclitante para eficiência e segurança da atividade administrativa, da mesma forma, a repristinação do Decreto 8.789/2016 seria inconsistente e temerária uma vez que os dados eram compartilhados de forma automática entre os órgãos do Poder Público e, sobretudo, havia uma certa omissão do legislador anterior em relação a proteção de dados pessoais.

Portanto, o Min. Gilmar Mendes entendeu por aplicar a técnica interpretativa de forma intermediária, conservando o texto do Decreto 10.046/2019 referente a todos os dispositivos contidos nele que se encontram em conformidade ao texto constitucional, reafirmando a força normativa da Constituição Federal de 1988.

Nesse itinerário, o min. Gilmar Mendes, com vistas a afastar interpretações deturpadas do Decreto impugnado, confere ao seu art. 3, I, onde discorre sobre "a informação do Estado", a leitura restrita às informações gerais do Estado, excluindo os atributos da personalidade ou aqueles inerentes ao cidadão.

Ainda no mesmo dispositivo, a expressão "compartilhada da forma mais ampla possível, deverá compreender tão somente as "informações relativas ao funcionamento do aparelho estatal". Por outro lado, quantos às informações de cunho pessoal, o compartilhamento deve submeter-se ao crivo e rigor da LGPD.

Em relação ao argumento da União quanto o tratamento de dados pelo Sistema Brasileiro de Inteligência com fulcro no Decreto de 2019 e LGPD, enfatiza que a própria lei de proteção de dados, em seu art.4º, III, dispõe que, para soberania nacional, deve-se criar legislação específica sempre observando o regulamentado pela Lei 13.709/2018

O relator ainda salienta que não é justo e, sequer, razoável a operação das repartições públicas com aparelhos e instrumentos defasados enquanto há uma

ISSN 2763-8448

intensa e exponencial evolução da sociedade moderna. A renúncia à tecnologia acarreta um aparelho estatal obsoleto e arcaico, contribuindo para a ineficiência administrativa.

Contudo, essa modernização dos serviços públicos, obviamente, não deve ser realizada de qualquer forma, sob descumprimento do princípio da legalidade. Trata-se de uma adequação à evolução tecnológica para atender às crescentes demandas da sociedade civil de forma eficaz e, principalmente, em conformidade com os fundamentos constitucionais.

Um exemplo do acórdão acerca da adequação tecnológica é a Portaria MTP 220, de 2 de fevereiro de 2022 em que há a dispensa da prova de vida do Instituto Nacional do Seguro Social (INSS) de forma presencial. Através do cruzamento de informações que a Administração Pública já detém, os segurados e beneficiários do INSS não precisam comparecer presencialmente às agências para comprovar que estão vivos e, ao mesmo tempo, combatendo-se potenciais fraudes.

Diante do exposto, o ministro relator considera que o Decreto 10.046/2019 interpretado à luz da LGPD não possui controvérsias ao instituir o Cadastro Base do Cidadão. Este, basicamente, constitui-se como um cadastro base necessário para intercomunicação do fluxo de dados entre os órgãos da administração.

Sobre o Comitê Central de Governança de Dados, é necessária uma maior análise acerca da composição do colegiado e indicação de seus membros. Aludindo às perspectivas internacionais, o acórdão demonstra que outras nações adotaram a sistemática de instituir autoridades administrativas para a proteção de dados pessoais, contudo, com maior rigorosidade quanto à composição multissetorial, atribuindo participação da sociedade civil e *experts*.

Assim, o min. Gilmar Mendes assevera “a necessidade de estruturar essas entidades a partir de uma composição plural e democrática, aberta, em alguma medida, a constante diálogo com a sociedade civil”. Logo, o Decreto 10.046/2019, ao designar a ocupação do Comitê Central de Governança de Dados com exclusividade a representantes da Administração Pública Federal, podia abalar a LGPD e, assim, violando o regime democrático, afeta a consolidação do direito à proteção de dados pessoais e a imagem nacional perante o âmbito internacional.

A estruturação concatenada de uma legislação, autoridades competentes e ferramentas que regulamentem a proteção de dados pessoais possui grande impacto

ISSN 2763-8448

para a imagem do Brasil nas relações internacionais. Exemplifica-se esse raciocínio através das organizações internacionais, como Organização para a Cooperação e Desenvolvimento Econômico (OCDE), observam criteriosamente aqueles que solicitam seu ingresso à entidade, inspecionando as legislações, órgãos e outros padrões.

Além da multissetorialidade, questiona-se a estruturação do Comitê já que, segundo o relator, "desarticula um mecanismo que é fundamental para o fortalecimento das salvaguardas previstas na LGPD".

Em síntese, houve o conhecimento da ADI e ADPF, julgando parcialmente procedentes os pedidos. Reconheceu-se a inconstitucionalidade do art. 22 do Decreto nº 10.046/2019, mantendo a estrutura do Comitê por um prazo de 60 dias a partir da publicação para adequação do texto normativo.

A Suprema Corte, ainda, atribuiu interpretação a determinados pontos do regulamento, definindo seis principais tópicos. À priori, o compartilhamento de dados pessoais entre os órgãos da Administração Pública deve estar em consonância com o princípio da finalidade (*vide* art. 6º, inciso I, da Lei 13.709/2018), adotando métodos legítimos, específicos e explícitos para as operações de tratamento de dados, o qual, consoante o princípio da adequação (art. 6º, inciso II), deve ser compatível com as finalidades devidamente apresentadas ao titular.

Essas operações, ainda, devem limitar-se ao mínimo necessário de acordo com o princípio da necessidade (art. 6º, inciso III), sem, evidentemente, haver excessos e cumprir todos os requisitos, garantias e procedimentos elencados pela LGPD no que diz respeito ao âmbito do poder público.

Outrossim, o compartilhamento no setor público precisa obrigatória e minuciosamente o que determina o art. 23 da LGPD, publicizando os atos e práticas utilizadas para execução das operações de tratamento conforme dispõe a Autoridade Nacional de Proteção de Dados.

Cabe ao Comitê Central de Governança de Dados, por sua vez, no exercício de suas competências definidas no art. 21, incisos VI, VII, e VIII, do Decreto nº10.046/2019, dispor sobre mecanismos de controle de acesso ao Cadastro Base do Cidadão, concedendo esse acesso tão somente a órgãos e entidades que, de fato, comprovarem a necessidade de acessar o referido banco de dados e o interesse público.

ISSN 2763-8448

Deve-se também justificar a inclusão de dados pessoais na base através dos princípios da proporcionalidade, razoabilidade e os postulados da LGPD assim como a escolha das bases temáticas.

Além disso, o Comitê deve instituir medidas de segurança com objetivos de, em hipótese de vazamento de dados, evitar ou minimizar os impactos e efeitos gerados, assim como desenvolver um sistema eletrônico com o registro de acesso para fins de responsabilização em situações de abuso.

Quanto as atividades de inteligências, essas devem observar a legislação específica que aborda sobre o compartilhamento de informações de cunho pessoal e os requisitos dispostos pelo julgamento da ADI 6.529, sendo eles: a adoção de medidas proporcionais e necessárias ao atendimento do interesse público, a propositura de uma procedimento administrativo formal, a utilização de sistema eletrônico responsável por registrar todo e qualquer acesso às bases e a observâncias aos pressupostos da LGPD no que diz respeito ao meio público.

Em circunstâncias de abusos e vazamento de informações pessoais, a responsabilidade civil do Estado será evocada para sanar os danos sofridos pelos titulares com fulcro nos arts. 42 e seguintes da Lei nº 13.709/2019, bem como o direito de regresso em face dos servidores públicos e agentes políticos que praticarem o ilícito culposa ou dolosamente. Sendo uma prática dolosa ao dever de publicidade, a responsabilização ocorrerá mediante ato de improbidade administrativa de acordo com o art. 11, inciso IV, da Lei nº 8.429/92.

8. LIMITES DA ADMINISTRAÇÃO PÚBLICA NO COMPARTILHAMENTO DE DADOS PESSOAIS SENSÍVEIS

Em um cenário de intenso desenvolvimento digital e consequente virtualização e adequação do Poder Público, surge uma fervorosa discussão que se bifurca em dois pensamentos antagônicos: o primeiro é referente a eficiência e desburocratização dos serviços públicos; e a segunda condiz aos potenciais riscos.

Gonçalves e Varella (2018) acrescentam ainda que a Administração Pública enfrenta um profundo desafio em equilibrar a aplicação da Lei de Acesso à Informação e assegurar a proteção de dados pessoais.

ISSN 2763-8448

O tratamento de dados pessoais proveniente do Poder Público está previsto no no capítulo IV da LGPD. Este capítulo divide-se em duas seções: a primeira apresenta as regras para discernir o tratamento e a segunda versa sobre a responsabilidade (Brasil, 2018).

Tendo em vista a autodeterminação informativa, essencialmente o ato administrativo acerca do tratamento de dados pessoais deve observar os princípios elencados no art. 6 º da LGPD, sobretudo, a finalidade, adequação e necessidade. Tratam-se de princípios que são fundamentais para nortear o tratamento de dados pessoais, exigindo fundamentação e estabelecendo limitações e consequências para ilicitudes.

A finalidade é aplicada sobre o tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem tratamento posterior. Ademais, a finalidade da coleta deve ser sempre cientificada e possui forte vínculo com o princípio da utilização não abusiva (Doneda *et al*, 2021).

Nos dizeres de Flôres e Silva (2023), o titular possui o direito ser cientificado de como suas informações estão sendo utilizadas nas operações de tratamento, evidenciando que, em casos de abusos, os agentes de tratamento devem ser responsabilizados.

Por sua vez, a adequação é disposta no sentido de compatibilidade do tratamento com as finalidades. Nessa senda, entende-se que deve possuir um mínimo de coerência entre o tratamento e a finalidade proposta (Brasil, 2018). Por fim, a necessidade como estabelecimento de um mínimo necessário para basear as finalidades sob o crivo da proporcionalidade e razoabilidade (Brasil, 2018).

Como exposto anteriormente, os dados pessoais sensíveis estão estritamente vinculados ao princípio da dignidade humana. A violação aos dados sensíveis, por consectário lógico, demonstra uma desobediência à dignidade da pessoa humana.

Logo, nota-se que é necessária uma exposição precisa sobre a destinação dos dados pessoais do titular pelo agente de tratamento. Dessa forma, a Lei nº 13.709/2018, em seu art. 11, enfatiza que ninguém será obrigado a dispor dados sensíveis a outrem, isto é, deve haver um consentimento e autorização expressa para ensejar o tratamento, salvo exceções do inciso II (Brasil, 2018).

Esse consentimento do indivíduo atribui uma responsabilidade ao destinatário, *in casu*, o Poder Público quanto à coleta e armazenamento de forma segura dos

ISSN 2763-8448

dados. Assim, a LGPD confere a responsabilização aos agentes que ministrarem de forma ilícita os dados pessoais já que, historicamente, o Estado sempre assumiu a posição hierárquico superior na relação titular-destinatário em face do interesse público (Flôres e Silva, 2023).

Diante o art. 26, §6º, é vedado ao ente público a transferência dos dados armazenados em seus bancos para instituições privadas, exceto na hipótese de convênios e contratos. Nessas hipóteses, a Autoridade Nacional de Dados Pessoais (ANDP) será cientificada para fiscalizar os atos das entidades (Brasil, 2018).

Para a LGPD, em seu art. 5º, inciso XIX, a autoridade nacional possui como objetivo zelar, implementar e fiscalizar o cumprimento da legislação em território nacional (Brasil, 2018).

Flôres e Silva (2023) ainda ressaltam que, em caso de descumprimento da legislação, as sanções serão aplicadas após conclusão do processo administrativo. O trâmite administrativo oportuniza o ente público de manifestar-se, assim, possibilitando o exercício do princípio da ampla defesa e do contraditório.

Comprovadas as infrações, a autoridade nacional deverá emitir um informe com as medidas cabíveis para combater as violações. Assim como poderá solicitar um relatório com a descrição dos potenciais impactos e sugerir boas práticas (Brasil, 2018).

De mais a mais, o art. 46 da LGPD, por sua vez, estabelece o dever de segurança da informação no tratamento de dados pessoais e prevê que os agentes da operação devem estabelecer medidas de segurança, técnicas e administrativas (Brasil, 2018).

Observa-se que o dispositivo indica medidas distintas: de segurança, técnicas e administrativas. As medidas de segurança são responsáveis por evitar, além de possíveis vazamentos, tratamentos ilícitos ou inadequados; por fim, as medidas técnicas e medidas administrativas consistem na organização da segurança (Doneda *et al*, 2021).

Mesmo após o encerramento do tratamento, os agentes envolvidos na operação continuam sendo responsáveis por garantir e manter a segurança dos dados consoante previsto no art. 47 (Brasil, 2018).

No entanto, ocorrendo quaisquer incidentes que acarretem em danos relevantes e irreparáveis o agente deve comunicar a autoridade nacional, em prazo

ISSN 2763-8448

razoável previamente definido pela autoridade, informando as informações dos titulares sob risco, as medidas de segurança adotas e outras com a finalidade de reverter o minimizar os impactos do incidente e, em caso de comunicação tardia, a motivação da demora, etc (Brasil, 2018).

9. CONSIDERAÇÕES FINAIS

No Brasil, antes da promulgação da Lei Geral de Proteção de Dados (LGPD), o tratamento de dados pessoais era abordado de forma indireta e esparsa no Código de Defesa do Consumidor (CDC), na Lei do Cadastro Positivo (Lei nº 12.414/2011), no Marco Civil da Internet e na Constituição Federal de 1988 por meio do direito à privacidade. Somente em 2010 uma legislação brasileira específica foi projetada e promulgada em 2018.

Ademais, antes de entender o conceito de dados pessoais e, inclusive, sensíveis, é necessário compreender três principais conceitos acerca da temática, quais sejam: titular, consentimento e tratamento. Extrai-se dessas terminologias a relação trilateral entre o titular (sujeito ativo), objeto e o destinatário (sujeito passivo).

Os dados pessoais, por sua vez, consistem no conjunto de informações da pessoa natural identificada ou identificável. Além disso, a sua subespécie, dados pessoais sensíveis, consiste em um conjunto de informações inerentes à personalidade do indivíduo que, sem as devidas limitações ao agente de tratamento, resultam em danos irreparáveis tanto para a segurança de um indivíduo como para sociedade civil.

Acerca do tratamento dos dados, a legislação prevê algumas hipóteses para sua execução, tais como: o consentimento, o legítimo interesse e outras elencadas pelo art. 7º da LGPD. Não obstante, ressalta-se que, quanto aos dados sensíveis, não há aplicação do legítimo interesse.

Em julgamento histórico do Supremo Tribunal Federal (STF), houve o reconhecimento da proteção de dados pessoais como um direito fundamental autônomo e independente do direito à privacidade, bem como a autodeterminação informativa.

ISSN 2763-8448

Além do mais, assim como a LGPD assegura a proteção de dados, a Lei nº 12.527 de 2011 tutela o acesso à informação. Dessa forma, uma divergência de direitos fundamentais é perceptível: enquanto um protege as informações, o outro possibilita a transparência e acesso a essas informações. Nota-se, portanto, uma colisão entre direitos.

Diante esse impasse, analogamente aos dizeres de Robert Alexy com a colisão de princípios, enfatiza-se que não há direito absoluto, sendo necessário, portanto, o sopesamento entre eles e, assim, prevalecendo aquele que melhor adequa-se ao caso concreto.

Na análise do Decreto nº 8.789 de 2016 e do Decreto nº 10.046 de 2019, verifica-se que este é uma reprodução daquele com algumas pequenas distinções, principalmente, no que diz respeito a expansão da governança, ao nível de compartilhamento de dados pessoais e a instituição do Comitê Central de Governança de Dados. O ato administrativo de 2019 abrange a governança do compartilhamento de dados para os poderes legislativo e judiciário, estabelece três níveis de compartilhamento (amplo, restrito e específico) e institui um comitê.

Contudo, antes das alterações posteriores à sua promulgação, percebe-se algumas inconsistências do decreto em relação à LGPD e a Constituição da República Federativa do Brasil. Tais inconsistências ficam evidenciadas, sobretudo, na composição do Comitê, que se limitava a tão somente membros da Administração Pública Federal.

Tendo em vista outras inconsistências, o Partido Socialista Brasileiro (PSB) e o Conselho Federal da Ordem dos Advogados do Brasil (CFOAB) ajuizaram respectivamente a ADPF 695 e ADI 6.649. A partir da análise dessas duas ações, o relator, Min. Gilmar Mendes, proferiu um voto conjunto, entendendo que a retirada por completo do decreto resultaria em danos graves ao ordenamento jurídico brasileiro já que a legislação anterior regulava o compartilhamento automático.

Portanto, a técnica interpretativa foi utilizada para embasar a fundamentação do acórdão, preservando partes do texto normativo e adequando o dispositivo aos preceitos constitucionais. Não obstante, especificamente, quanto ao Comitê instituído pelo decreto, entendeu-se por sua inconstitucionalidade justamente por não haver em sua composição uma participação plural de setores da sociedade civil, contrariando o regime democrático brasileiro.

ISSN 2763-8448

A importância de uma multissetorialidade em entidades, como o Comitê, possui uma extrema importância e relevância para a imagem do país no âmbito das relações internacionais. Organizações de diversos países observam criteriosa e rigorosamente as legislações, autoridades e ferramentas daquelas nações que solicitaram ingresso, sob pena de romper ou dificultar relações e negociações.

Essa observância à infraestrutura torna-se ainda mais relevante quando a temática envolve os dados pessoais, visto que são considerados pela doutrina majoritária como uma fonte de riqueza. Esse conjunto de informações, em uma era digital com crescimento tecnológico exponencial, possuem grande valor econômico já que podem, por exemplo, criar um perfil de indivíduo para o mercado de consumo e compor bases de dados, fomentando sistemas de *Big Data* e de inteligência artificial.

Além da relevância patrimonial, o tratamento adequado dessas informações é crucial para a preservação de um regime democrático. A forma como o tratamento dos dados, principalmente, sensíveis dispõe sobre o método de compartilhamento revela como um Estado atua sobre o seu povo: ou sendo um ente estatal autoritário que utiliza esses dados como forma de controle social ou que assegura a proteção desses dados em prol de uma democracia.

Nesse sentido, é necessário que o tratamento dos dados pessoais, sobretudo, sensíveis deve estar em harmonia com os princípios constitucionais e outros elencados pela LGPD, em especial, a finalidade, adequação e necessidade. É imprescindível que a Administração Pública seja transparente quanto a finalidade que atribui para o tratamento para evitar potenciais práticas abusivas, devendo respeitar o instituto do consentimento, explicitando sua razoabilidade, bem como correlacionar um mínimo de coerência entre a operação e sua finalidade, assegurando a dignidade humana.

O tratamento inadequado fulcrado em um dispositivo legal, como por exemplo foi evidenciado pelo Laboratório de Políticas Públicas e Internet (LAPIN), acarreta, além da insegurança jurídica, danos irreparáveis para o titular dos dados pessoais sensíveis uma vez que, por conta da sua natureza e peculiaridade, contêm informações confidenciais referentes ao particular de cada indivíduo. Dessa forma, violando o consentimento e as liberdades de escolhas do titular quanto dispor e, sobretudo, ser cientificado acerca do tratamento de seus dados, há violação expressa e grave ao princípio da dignidade da pessoa humana.

ISSN 2763-8448

Para além dos princípios, a LGPD ainda elenca uma série de requisitos embasados pelo princípio da prevenção para evitar o risco à segurança das informações. Essas medidas, pautadas na segurança e boas práticas, objetivam evitar, além dos vazamentos, práticas ilícitas ou inadequadas quanto a execução do tratamento de dados.

REFERÊNCIAS

ALVAREZ, Cezar. Um programa para a transformação digital do Brasil. ObservaBR: Caminhos da Reconstrução e Transformação do Brasil. Fundação Perseu Abramo, 2020. Disponível em: https://fpabramo.org.br/observabr/2020/10/21/um-programa-para-a-transformacao-digital-do-brasil/. Acesso em: 13 dez. 2023

ARAGÃO, João Carlos Medeiros de. Choque entre direitos fundamentais: Consenso ou controvérsia? **Revista de Informação Legislativa**. a. 48, nº 189, p.259-268, 2011. Disponível em:https://www2.senado.leg.br/bdsf/bitstream/handle/id/242874/000910807.pdf?sequence=1&isAllowed=y. Acesso em: 13 dez. 2023.

BRASIL. **Constituição Federal.** Brasília: Senado Federal, 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 13 dez. 2023.

BRASIL. Emenda Constitucional nº 115, de 10 de fevereiro de 2022. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. **Diário Oficial da República Federativa do Brasil**, 10 de fevereiro de 2022. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm#:~:text=EMENDA%20CONSTITUCIONAL%20Nº%20115%2C%20DE,e%20tratamento%20de%20dados%20pessoais. Acesso em: 13 dez. 2023.

BRASIL. 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. **Diário Oficial da República Federativa do Brasil**, 18 de novembro de 2011. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 13 dez. 2023

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Institui a Lei Geral de Proteção de Dados (LGPD). **Diário Oficial da República Federativa do Brasil**, 15 de agosto de 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 13 dez. 2023.

ISSN 2763-8448

BRASIL. Decreto nº 8.789, de 29 de junho de 2016. Dispõe sobre o compartilhamento de bases de dados na administração pública federal. Diário Oficial da República Federativa do Brasil, DF, 29 de junho de 2016. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8789.htm. Acesso em: 13 dez. 2023.

BRASIL. Decreto nº 10.046, de 9 de outubro de 2019. Dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro de Base do Cidadão e o Comitê Central de Governança de Dados. Diário Oficial da República Federativa do Brasil, Brasília, DF, 9 de out. de 2019. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/d10046.htm. Acesso em: 13 dez. 2023.

BRASIL. Decreto nº 11.266, de 25 de novembro de 2022. Altera o Decreto nº10.046, de 9 de outubro de 2019, que dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê de Governança de Dados. Diário Oficial da República Federativa do Brasil, DF, 25 de novembro de 2022. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2022/Decreto/D11266.htm. Acesso em: 13 dez. 2023.

BRASIL. Superior Tribunal Federal. **Arguição de Descumprimento de Preceito Fundamental nº 695 e Ação Direta de Inconstitucionalidade nº 6649/DF**. Relator: Ministro Gilmar Mendes. Disponível em: https://images.jota.info/wp-content/uploads/2022/09/voto-adi-6649-e-adpf-695-1.pdf. Acesso em: 13 dez. 2023.

CUNHA JÚNIOR, Dirley da. **Curso de direito constitucional**. 13 ed. Salvador: JusPODIVM, 2018.

DONEDA, D. *et al*. **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021. Disponível: https://integrada.minhabiblioteca.com.br/reader/books/9788530992200/epubcfi/6/10[%3Bvnd.vst.idref%3Dhtml4]!/4/24/3:280[Ltd%2Ca.]. Acesso em: 13 dez. 2023.

FERRAZ JÚNIOR, T. S. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. **Revista da Faculdade de Direito, Universidade de São Paulo**, *[S. l.]*, v. 88, p. 439-459, 1993. Disponível em: https://www.revistas.usp.br/rfdusp/article/view/67231. Acesso em: Acesso em: 13 dez. 2023.

FLÔRES, M. R. de; SILVA, R. L. da . Desafios e perspectivas da proteção de dados pessoais sensíveis em poder da administração pública: entre o dever público de informar e o direito do cidadão de ser tutelado. **Revista de Direito**, *[S. l.]*, v. 12, n. 02, p. 01–34, 2020. DOI: 10.32361/2020120210327. Disponível em: https://periodicos.ufv.br/revistadir/article/view/10327. Acesso em: 13 dez. 2023

GONÇALVES, Tânia Carolina Nunes Machado; VARELLA, Marcelo D. Os desafios da Administração Pública na disponibilização de dados sensíveis. **Revista Direito GV**, [S.l.], v. 14, n. 2, p. 513-536, set. 2018. ISSN 2317-6172. Disponível em: http://bibliotecadigital.fgv.br/ojs/index.php/revdireitogv/article/view/77110/73916. Acesso em: 13 dez. 2023.

LUGATI, L. N.; ALMEIDA, J. E. de. A LGPD e a construção de uma cultura de proteção de dados. **Revista de Direito**, [S. l.], v. 14, n. 01, p. 01–20, 2022. DOI:

ISSN 2763-8448

10.32361/2022140113764. Disponível em:https://periodicos.ufv.br/revistadir/article/view/13764. Acesso em: 13 dez. 2023.

MARCATO, Antonio Carlos *et al*. **Código de Processo civil interpretado**. 1ª ed. São Paulo: Atlas, 2022.

PINHEIRO, Patrícia Peck. **Proteção de dados pessoais: comentários à Lei n. 13.709/2018 (LGPD)**. 2ª ed. São Paulo: Saraiva Educação, 2020.

SARLET, G. B. S.; RUARO, R. L. A proteção de dados sensíveis no sistema normativo brasileiro sob enfoque da Lei Geral de Proteção de Dados – L.13.709/2018. **Revista Direitos Fundamentais & amp; Democracia**, [S. l.], v. 26, n. 2, p. 81–106, 2021a. DOI:10.25192/issn.1982-0496.rdfd.v26i22172. Disponível em: https://revistaeletronicardfd.unibrasil.com.br/index.php/rdfd/article/view/2172. Acesso em: 13 dez. 2023.

SARLET, Ingo Wolfgang. O Direito Fundamental à Proteção de Dados Pessoais na Constituição Federal Brasileira de 1988. **Revista Privacidade e Proteção de Dados (*Privacy and Data Protection Magazine*)**, v.1, n.1, p. 12-49, 2021b. Disponível em: https://repositorio.pucrs.br/dspace/handle/10923/18868. Acesso em: 13 dez. 2023

SARLET, Ingo Wolfgang. As dimensões da dignidade da pessoa humana: construindo uma compreensão jurídico-constitucional necessária e possível. BDJur: Biblioteca Digital Jurídica, 2007. Disponível em: https://bdjur.stj.jus.br/jspui/handle/2011/27252. Acesso em: 13 dez. 2023

SOUSA, R. P. M. de; BARRANCOS, J. E.; MAIA, M. E. Acesso à informação e ao tratamento de dados pessoais pelo Poder Público. **Informação & amp; Sociedade: Estudos**, [S. l.], v. 29, n. 1, p. 237-251, 2019. Disponível em: https://periodicos.ufpb.br/ojs2/index.php/ies/article/view/44485/223. Acesso em: 13 dez. 2023

Recebido em (Received in): 19/04/2024.
Aceito em (Approved in): 29/06/2024.