DADOS PESSOAIS NO BRASIL: NORMATIVAS E DIÁLOGOS INSTITUCIONAIS RUMO À ATUAL LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

Wagner de Oliveira Rodrigues[62]

Vanderson Barbosa da Rocha[63]

RESUMO

O presente artigo analisa o cenário da proteção legislativa dos dados das pessoas naturais no Brasil com o advento da Lei Geral de Proteção de Dados, por meio do estudo dos aspectos gerais desta norma e a sua relação com a Administração Pública e o princípio da transparência pública. Para tanto foi feita extensa pesquisa bibliográfica e jurisprudencial a respeito da tutela jurídica da privacidade e dos dados pessoais na sociedade da informação – perfilhando-se um panorama global acerca das normas de proteção de dados pessoais e o arcabouço normativo no Brasil até a sanção da Lei Geral de Proteção de Dados. Ao fim, analisa os aspectos gerais desta norma e sua relação com a Administração Pública, com destaque para a Agência Nacional de Proteção de Dados, e estuda a existência de um possível conflito entre a norma em estudo e a Lei de Acesso à Informação.

PALAVRAS-CHAVE: Dados pessoais. Lei Geral de Proteção de Dados. Transparência Pública. Acesso à Informação.

ABSTRACT

The present paper analyze the scenario of the law protection of the persons data in Brazil by "General Data Protection Act", through the general aspects of this, its relationship with the Brazilian Public Administration and the transparency public's principle. Here using the bibliographic research methodology, discusses the legal protection of privacy and personal data in the information society traces a global panorama about the rules like this and presents the legal framework in Brazil until the sanction of the "General Data Protection Act" running for general aspects of this standard and its relationship with the Brazilian State, with focus on the National Data Protection Agency. Finally analyzes the existence of a possible conflict between the standard study and the Access to Information Act.

KEYWORDS: Person data. General Data Protection Act. Public Transparency. Information access

INTRODUÇÃO

A grande conectividade do mundo contemporâneo gera a circulação de um expressivo volume de dados acerca de pessoas envolvidas nas mais diversas relações, sejam elas consumeristas, trabalhistas ou relacionadas ao exercício de deveres e direitos em face do Estado. Neste cenário de sociedade da informação, o dado já tem sido tratado como uma das mais valiosas *commodities* e o seu tratamento, quando efetuado de forma indevida, pode causar diversos danos aos seus titulares. Diante disso, iniciou-se um

[62] Professor Adjunto lotado no Departamento de Ciências Jurídicas na Universidade Estadual de Santa Cruz (UESC), em Ilhéus, Bahia. Doutor em Ciências Jurídicas e Sociais (PPGSD - Universidade Federal Fluminense) na linha de Conflitos Socioambientais, Rurais e Urbanos. Líder do Grupo CNPq de Pesquisa em Direitos Humanos e Fundamentais na UESC. (GPDH/UESC). Diretor Sindical na ADUSC - Associação dos Docentes da UESC. Membro da Rede ODS-BRASIL.

[63] Graduando em Direito pela Universidade Estadual de Santa Cruz (UESC).

movimento mundial, com a finalidade de tutelar juridicamente os dados das pessoas naturais, que resultou na criação de normas específicas acerca do tema nos quatro cantos do mundo. No Brasil, em que pese a existência de dispositivos que tratam do assunto em normas setoriais anteriores, a lei específica que versa sobre o tema só foi sancionada em 2018, após longa discussão política e forte pressão dos atores econômicos internacionais.

Conhecida popularmente como Lei Geral de Proteção de Dados (LGPD), a Lei 13.709 de 14 de agosto de 2018 regulamenta o tratamento de dados pessoais, quaisquer sejam os meios em que estejam armazenados e pessoas que o detenham, inclusive entes integrantes da Administração Pública, com a finalidade de proteger os direitos fundamentais da privacidade, liberdade e livre desenvolvimento da personalidade da pessoa natural. O Poder Público ocupa papel de destaque na LGPD, visto que, além do fato de seus entes integrantes serem os maiores agentes de tratamento de dados pessoais no Brasil, a efetividade desta norma depende diretamente da sua atuação, por meio da Agência Nacional de Proteção de Dados, na fiscalização do seu cumprimento, edição de regulamentos a ela atribuídos e aplicação de sanções em situações decorrentes de tratamentos indevidos.

Além disso, com a novidade da norma, gera-se uma dúvida acerca do possível conflito do diploma legal de proteção dos dados pessoais com o regramento da transparência pública nas relações entre as pessoas naturais e a Administração Pública, cujo principal instrumento de concretização é a Lei 12.527/2011, conhecida popularmente como Lei de Acesso à Informação (LAI). Nesse cenário, objetivamos neste trabalho efetuar, sob a égide dos preceitos jurídicos, a análise da evolução da proteção de dados das pessoas naturais no mundo e no Brasil, cuja culminância se deu com o advento da LGPD, sobre a qual tratamos dos aspectos gerais, regramentos para a Administração Pública e análise da existência ou não de conflito com a LAI. O enfoque deste trabalho sobre as leis de proteções de dados pessoais no mundo, com destaque para a LGPD e sua relação com a Administração Pública, se faz relevante pelo fato da novidade da lei no ordenamento jurídico brasileiro e o estabelecimento, por ela, de papéis importantes para o Poder Público, além da possível interferência na transparência pública. Quanto à metodologia utilizada neste artigo, foi utilizada a revisão bibliográfica com a consulta de diversas fontes – tais como livros, periódicos, artigos e acórdãos, nos quais a temática foi debatida por magistrados e estudiosos do tema – que foram devidamente analisadas e utilizadas com os fins propostos para o desenvolvimento deste trabalho.

1. ESTADO E DIREITO NA SOCIEDADE DA INFORMAÇÃO

Desde meados do século XX a sociedade tem experimentado um processo de grandes transformações tecnológicas. Os avanços em robótica, nanotecnologia e conectividade provocaram mudanças radicais nas relações sociais. Notícias que levavam meses para chegar ao seu destino hoje são entregues em fração de segundos. Grupos de trabalho que só eram viáveis com a presença de todos os membros no mesmo espaço físico atualmente podem ser realizados virtualmente.

Documentos públicos que levavam tempo para ser emitidos podem ser obtidos com um simples clique. Todas essas inovações só se tornaram possíveis por conta da melhoria da capacidade de transmissão, armazenamento e processamento de dados.A rápida evolução da capacidade de armazenamento de dados em meios físicos cada vez menores ou até mesmo em "nuvem" é o alicerce de toda essa revolução social. Há menos de trinta anos, o meio comum de guardar os dados era um dispositivo chamado "disquete", que ocupava "grande" espaço físico e tinha ínfimo espaço de armazenamento quando comparado com as tecnologias atuais.

Diante deste avanço se fez necessário o aperfeiçoamento das tecnologias de transmissão e o devido processamento de dados para fornecer informações. Com isso, foram desenvolvidas sofisticadas ferramentas de tecnologia da informação e comunicação e métodos de inteligência de dados, conhecidos como *Big Data*, que têm sido cada vez mais utilizadas por pessoas naturais e jurídicas. Por meio da utilização dessas ferramentas, as entidades ou até mesmo as pessoas naturais têm o poder de auferir valiosas informações acerca de indivíduos com os quais mantêm relacionamento e, de alguma forma, armazenam dados sobre eles. Com isso, empresas têm hoje a capacidade de analisar o comportamento dos seus clientes e personalizar as ofertas, empregadores podem atuar na gestão dos seus empregados e Estados podem coletar vários tipos de informações acerca da sua população.

Já os Estados são, sem sombra de dúvidas, desde os mais intervencionistas aos liberais, os entes que possuem as bases com o mais expressivo volume de dados acerca das pessoas naturais. Os indivíduos estabelecem desde a sua concepção uma ligação perene com os Estados que perdura até mesmo após a sua morte. No âmbito dessa relação são coletados inúmeros dados acerca de cada pessoa natural que povoam os poderosos bancos de dados estatais. Assim, este massivo e crescente armazenamento de dados das pessoas naturais por outras pessoas, empresas ou entes estatais com que se relacionam torna cada vez mais emergentes os riscos do uso indevido das informações. Nas palavras de Silva (2005, p. 209-210):

> O intenso desenvolvimento de complexa rede de fichários eletrônicos, especialmente sobre dados pessoais, constitui poderosa ameaça à privacidade das pessoas. O amplo sistema de informações

> computadorizadas gera um processo de esquadrinhamento das pessoas, que ficam com sua individualidade inteiramente devassada. O perigo é tão maior quanto mais a utilização da informática facilita a interconexão dos fichários com a possibilidade de formar grandes bancos de dados que desvendem a vida dos indivíduos, sem sua autorização e até sem seu conhecimento.

Diante desse cenário, visto que o cerne da sociedade da informação é o compartilhamento de dados, se faz necessário o aprimoramento da tutela dos direitos à privacidade e dos instrumentos legais de proteção de dados das pessoas naturais, a fim de que estes sejam harmonizados com o acesso à informação e os indivíduos sejam protegidos contra a redução exagerada das suas intimidades (LISBOA, 2019).

No contexto do Brasil, e dado o ocaso da Carta Magna de 1988 a contemplar inúmeros direitos fundamentais, não seria diferente a proteção da privacidade como um elemento essencial de promoção da dignidade humana. Ainda assim, é salutar dizer que o conceito de privacidade é aberto e pode variar de acordo com o tempo, região geográfica, cultura ou com as características de cada pessoa.

Por um longo período, a privacidade foi entendida como o direito de ser deixado só. Na sociedade contemporânea, entretanto, diante da "hiperconectividade" essa noção se mostrou insuficiente e foi percebida a necessidade de se tutelar juridicamente o instituto. Corroborando-se este pensamento, através da lição de Doneda (2006, p. 91):

> Certamente não havia lugar para a tutela jurídica da privacidade em sociedades que conferiam a sua regulação a outros mecanismos – fosse uma rígida hierarquia social ou então a arquitetura dos espaços públicos e privados; fosse porque as eventuais pretensões a este respeito estivessem neutralizadas por um ordenamento jurídico de cunho corporativo ou patrimonialista; ou fosse então porque, em sociedades para as quais a privacidade representasse não mais que um sentimento subjetivo, ela não merecesse tutela.

A tutela jurídica da privacidade como um direito fundamental na forma em que conhecemos atualmente teve a sua primeira manifestação codificada na Declaração Universal dos Direitos Humanos, em 1948, a qual dispõe em seu artigo 12º que "ninguém será sujeito a interferências na sua vida privada, na sua família, no seu lar ou na sua correspondência, nem a ataques a sua honra e reputação. Todo o homem tem direito à proteção da lei contra tais interferências ou ataque" (ORGANIZAÇÃO DAS NAÇÕES UNIDAS, 2009, p. 5). Nota-se nesse preceito legal o distanciamento com antigo entendimento de privacidade que se limitava ao direito de ser deixado só e a ampliação da cobertura desse instituto.

No Brasil a doutrina majoritária preleciona que o direito à privacidade engloba os direitos fundamentais da seara privada,

íntima e da personalidade consagrados pela Constituição da República Federativa do Brasil (CRFB) de 1988. Logo, de acordo com esse entendimento, no ordenamento jurídico brasileiro a privacidade consiste no universo de informações sobre o indivíduo, e somente a este cabe a divulgação ou manutenção e sigilo dos mesmos. Assim, em Moraes (2020, p. 76), se contextualiza o seguinte:

> A defesa da privacidade deve proteger o homem contra: (a) interferência em sua vida privada, familiar e doméstica; (b) a ingerência em sua integridade física ou mental, ou em sua liberdade intelectual e moral; (c) os ataques à sua honra e reputação; (d) sua colocação em perspectiva falsa; (e) a comunicação de fatos relevantes e embaraçosos relativos à sua intimidade; (f) o uso de seu nome, identidade e retrato; (g) a espionagem e a espreita; (h) a intervenção na correspondência; (i) a má utilização de informações escritas e orais; (j) a transmissão de informes dados ou recebidos em razão de segredo profissional.

Verifica-se, assim, que, apesar de nenhum direito ser absoluto ou instransponível, a atual Carta Magna brasileira destaca a relevância do direito à privacidade no seu rol de direitos fundamentais e em suas cláusulas pétreas. Ou seja, na sociedade da informação, a privacidade está umbilicalmente ligada à proteção dos dados pessoais e, com isso, verifica-se nas últimas décadas um movimento legislativo global para a garantia da proteção dos dados pessoais como um dos meios de tutela jurídica da privacidade. Em que pese a aproximação dos conceitos, é importante destacar que "[...] não se pode dizer que o direito à proteção dos dados pessoais se limita a "um aspecto do direito à privacidade, como se estivesse inteiramente nele contido." (QUEIROZ, 2019, p. 19).

Nesse sentido, Bioni (2020) destaca a autonomia do direito à proteção dos dados pessoais que confere ao titular, além do direito à não intervenção inerente à privacidade, acepção mais abrangente com tutela jurídica e âmbito de incidências específicos. Seguindo-se esta linha, em recente decisão, no âmbito do julgamento da Ação Direta de Inconstitucionalidade (ADI) 6.387, que questionava a constitucionalidade da Medida Provisória (MP) nº 954/2020, a qual previa, enquanto durasse a pandemia da COVID-19, o repasse obrigatório de dados dos clientes das operadoras de telefonia móvel e fixa para o Instituto Brasileiro de Geografia e Estatística (IBGE).

Resultado da análise deste caso, o Supremo Tribunal Federal (STF) decidiu pela inconstitucionalidade da norma e, historicamente, reconheceu a proteção de dados pessoais como direito fundamental autônomo. De acordo com o entendimento firmado pelo Egrégio Tribunal, a tutela do direito fundamental à proteção de dados vai além da delimitação de um espaço e ampara também os direitos à transparência, governança e sindicabilidade dos dados compreendidos num aspecto abrangente. Neste diapasão, a MP foi considerada

exorbitante, visto que previa o compartilhamento de extenso rol de dados sensíveis dos cidadãos e representava o eminente risco de danos irreparáveis à intimidade e ao sigilo da vida privada dos milhões de usuários do serviço de telefonia fixa e móvel (BRASIL, 2020).

2. DADOS PESSOAIS: O CONTEXTO DA PROTEÇÃO GLOBAL

Para compreender o panorama internacional da proteção legislativa dos dados pessoais, se faz necessário remeter ao histórico havido durante a Segunda Guerra Mundial. No decorrer do conflito os alemães nazistas se fizeram valer de diversos meios de violação da privacidade dos cidadãos nos territórios invadidos com a finalidade de manipular o comportamento dos indivíduos e, assim, perseguir minorias sociais como os judeus e os homossexuais. Tal exemplo demonstra quão nefasto pode ser o tratamento indevido de dados pessoais e deixou profundas cicatrizes em toda a sociedade, com destaque para alemã, e como consequência disso "[...] a proteção de dados se tornou uma obsessão jurídica na Alemanha." (CAMARGO, 2019, p. 221).

Foram justamente esses horrores cometidos em contextos bélicos que ensejaram os fatos políticos geradores para a feitura do documento "Declaração Universal dos Direitos Humanos", que é a grande matriz global, desde 1948, de inspiração para o panorama legislativo da proteção de dados. Neste diapasão, em 1950 foi editada a Convenção Europeia dos Direitos Humanos, que trouxe uma proteção extremamente relevante da privacidade do indivíduo em relação ao Estado, quando dispôs no item 2 do seu art. 8º que:

> Não pode haver ingerência da autoridade pública no exercício deste direito senão quando esta ingerência estiver prevista na lei e constituir uma providência que, numa sociedade democrática, seja necessária para a segurança nacional, para a segurança pública, para o bem-estar econômico do país, a defesa da ordem e a prevenção das infracções penais, a proteção da saúde ou da moral, ou a proteção dos direitos e das liberdades de terceiros.

Diante dessa necessidade de se tutelarem os dados, do crescente avanço tecnológico e do surgimento de uma economia globalizada com a evolução dos bancos de dados eletrônicos, a partir especialmente dos anos 1970, é que começaram a ser editados diplomas legislativos específicos para a proteção dos dados pessoais. Neste sentido, e para melhor organização do contexto geopolítico legislativo ao redor do globo, se fará uma rápida apresentação do que foi destaque nos seus principais países nos quatro cantos do mundo.

2.1 Europa

A Europa pode ser considerada o berço da proteção dos dados pessoais no planeta. A primeira lei regional específica na proteção de dados foi criada em 1970 na Alemanha, era denominada *Hessisches Datenschutzgesetz* e tinha como finalidade principal proteger os indivíduos de abusos estatais. Nos anos de 1973 e 1974 o Conselho da Europa editou, respectivamente, as Resoluções 22, que tratava da privacidade das pessoas físicas perante bancos eletrônicos de dados no setor privado, e 29, que tratava da proteção e privacidade das pessoas físicas perante bancos eletrônicos de dados no setor público (MACHADO, 2018).

Em seguida diversos países do continente, como França, Dinamarca e Suécia, editaram leis nacionais sobre a proteção de dados pessoais, e alguns deles, inclusive, trataram o assunto como matéria constitucional. Mas, diante do aprimoramento do setor informático e dos blocos econômicos, que teve como uma das consequências o aumento do volume de compartilhamento de dados nos atos de comércio transfronteiriço, em 1980 a Organização para a Cooperação e Desenvolvimento Econômico (OCDE) publicou diretrizes recomendatórias para a proteção da privacidade e dos fluxos transfronteiriços de dados pessoais. Sob uma forte influência dessas diretrizes, em 1981 o Conselho da Europa instituiu a Convenção 108, que consolidou as Resoluções 22 e 29 e é considerada o primeiro diploma legal transnacional acerca da proteção de dados pessoais (MACHADO, 2018).

Contudo, e com o passar do tempo, surgiu a necessidade de aperfeiçoamento da Convenção 108, por conta do aprimoramento nas tecnologias de bancos de dados e ferramentas de tecnologias da informação. Diante disso, a Comissão Europeia, provocada pelo Parlamento Europeu, editou a Diretiva nº 46 de 1995, que foi por mais de duas décadas o principal documento sobre proteção de dados pessoas e privacidade. Entretanto, a norma apenas traçava um objetivo geral, e os próprios Estados Membros deveriam se adequar por meio da edição de normas internas. Isso resultou em desarmonia e conflito entre as diversas legislações e, consequentemente, insegurança jurídica e inobservância do princípio fundamental à proteção de dados (ARAUJO; OLIVEIRA, 2015).

Perante esse cenário, se fez necessária a adoção de um Regulamento compulsório aos Estados Membros em substituição à Diretiva nº 46. Assim, em 2016 foi editado o Regulamento nº 679, conhecido como *General Data Protection Regulation* (GDPR), que entrou em vigência em 25 de maio de 2018 e passou a ser o principal diploma de proteção de dados pessoais na União Europeia (UE). O advento do GDPR é de suma importância para entender o tema, visto que:

> Este, por sua vez, ocasionou um efeito dominó, visto que passou a exigir que os demais países e as

> empresas que buscassem manter relações comerciais com a UE também deveriam ter uma legislação de mesmo nível que o GDPR. Isso porque o Estado que não possuísse lei de mesmo nível passaria a poder sofrer algum tipo de barreira econômica ou dificuldade de fazer negócios com os países da UE. Considerando o contexto econômico atual, esse é um luxo que a maioria das nações, especialmente as da América Latina não poderia se dar. (PINHEIRO, 2020, p. 18).

Nessa seara, visto que o GDPR é vinculante em todo o Espaço Econômico Europeu (EEE), que engloba os vinte e sete países integrantes da União Europeia e ainda Noruega, Islândia e Listenstaine, e extensível a todas as operações que envolvem dados pessoais efetuadas para fora do EEE, ou seja, todos os Estados e empresas que visem a manter relações comerciais com seus integrantes – que possuem enorme poder econômico – devem se adequar ao regulamento, diversos outros países buscaram adequar suas legislações de proteção de dados pessoais ao Regulamento com a finalidade de evitar sofrer barreiras negociais (MOLINARI; SEBASTIÁN; VÁZQUEZ, 2018).

2.2 Estados Unidos da América

Os Estados Unidos da América, ao contrário da Europa, talvez pela sua preponderante edição de leis locais, característica inerente de uma federação centrípeta, ainda não possuem uma lei nacional que discipline a proteção de dados pessoais. Entretanto, com a eleição de Joe Biden para presidente do país, há uma forte expectativa no avanço da aprovação do *Consumer Data Privacy and Security Act* (CDPSA), projeto que tramita no Congresso Nacional Americano e tem entre suas finalidades a de proteger os dados pessoais dos consumidores em todo o território nacional (REIS, 2021).

Enquanto não há o estabelecimento de uma lei federal, alguns estados americanos caminham para a instituição de leis estaduais de proteção de dados pessoais. O estado da Califórnia já aprovou em 2017 a sua norma denominada *California Consumer Privacy Act* (CCPA) que, durante o seu trâmite, contou com o forte apoio da então procuradora-geral do estado e atual vice-presidente Kamala Harris e, em março de 2021, a Virgínia se tornou o segundo estado americano a aprovar a sua lei de proteção de dados pessoais denominada *Virginia Consumer Data Privacy Act* (HALPERT, 2021).

Cumpre ressaltar também que o atentado ocorrido no país em 11 de setembro de 2001 resultou no endurecimento das medidas de segurança no país que, logicamente, envolvem a captura de dados pessoais. Entretanto, mostrou-se ainda mais eminente a necessidade de conciliação e equilíbrio entre o direito à segurança e à proteção dos dados das pessoas naturais – ainda que a segurança pública fosse uma

emergência internamente assaz (CASTRO, 2003).

2.3 Ásia

Em que pesem as diversas diferenças culturais, os principais países do continente asiático, em consonância com o que vem ocorrendo nas nações dos demais continentes, têm regulamentado e aperfeiçoado seus ordenamentos jurídicos com a finalidade de tutelar os dados pessoais das pessoas naturais. O Japão é um excelente exemplo desse movimento. Em 2003 o país editou uma lei específica de proteção de dados pessoais. No ano de 2010, em consequência dos avanços tecnológicos e com o fim de estabelecer sincronia com a legislação europeia, estabeleceu a denominada Emenda APPI, que dispõe sobre o compartilhamento de dados pessoais com terceiros, anonimização e prevenção de vazamentos. Além disso, foi criada uma autoridade reguladora de proteção de dados pessoais cujos dirigentes exercem suas funções com total independência. Recentemente, em 2019, o Japão e a União Europeia celebraram um acordo o qual foi chamado de maior espaço de circulação segura dos dados a nível mundial, que consiste basicamente num ambiente de transferência com alto nível de segurança de dados de pessoas naturais (CAMARGO; TAGLIAFERRO, 2020).

Já na China, em janeiro de 2021, entrou em vigor o Código Civil da República Popular da China que, entre seus ditames, regulamenta a privacidade e proteção dos dados pessoais. Além disso, está em discussão no país um projeto de lei específica para a proteção de dados pessoais que em bastante se assemelha com a GDPR. Paralelamente a este país, a Coreia do Sul instituiu, em 2011, uma das leis de proteção de dados pessoais mais rígidas do mundo, com controles ainda mais rigorosos do que as normas europeias e com a criação de duas autoridades de proteção de dados. Contudo, outros países asiáticos, como Índia, Malásia e Indonésia, embora ainda não possuam lei específica sobre a proteção de dados pessoais, já contam com projetos de lei acerca do tema em vias de aprovação (DALESE, 2021).

Com o advento da pandemia de COVID-19 e os rígidos sistemas de controle e rastreamento adotados por parte dos países asiáticos, com destaque para os monitoramentos pela tecnologia de geolocalização, geraram-se, ao redor do mundo, muitas dúvidas acerca da proteção dos dados pessoais naquele continente. Houve até a difusão de teorias conspiratórias, criadas por setores negacionistas da sociedade, as quais, absurdamente, afirmavam que o vírus causador da doença teria sido criado em laboratório e espalhado pela China com o fim de obter o controle sobre a vida dos indivíduos.

Ocorre que os países do continente asiático têm um histórico traumático de experiências com epidemias e naturalmente desenvolveram meios para combater precocemente o surgimento de novas ameaças e, sem sombra de dúvidas, o uso da tecnologia é um dos instrumentos mais eficazes. Não obstante o exposto, diante da dimensão da utilização dos dados pessoais com a finalidade de preservar a saúde coletiva em meio à pandemia, se faz necessário acompanhamento rigoroso ao longo dos próximos anos, a fim de garantir que os dados coletados não sejam utilizados para propósito diverso.

2.4 América Latina

No âmbito da América Latina, o primeiro país a instituir uma lei específica com a finalidade da proteção de dados foi o Chile, em 1999, com a norma denominada *Ley de Protección de Datos de Carácter Personal*, que limita o uso dos dados à finalidade informada no ato da coleta, garante aos titulares o direito de acessar as informações e prevê a responsabilidade dos controladores pelos danos causados aos titulares. Em 2018 o país incorporou ao seu rol de direitos fundamentais constitucionais o direito à proteção dos dados pessoais. Um ano depois, no ano 2000, a Argentina estatuiu a *Ley de Protección de los Datos Personales*, que regula o uso dos bancos de dados públicos e privados e limita o uso dos dados pessoais à finalidade para a qual houve o consentimento do titular. Além disso, a autoridade de proteção de dados do país, denominada *Agencia de Acceso a la Información Pública* (AAIP) detém o poder de editar disposições técnicas acerca do tema (BRASIL, 2015).

Logo em seguida o Paraguai editou a Lei 1.682/2001 com o objetivo de regulamentar a informação de caráter privado e a transparência dos bancos de dados de caráter público. Além disso, a norma proíbe a divulgação de dados sensíveis, que sejam individualizados ou individualizáveis ou versem sobre ligações raciais ou étnicas, preferências políticas, estado de saúde individual, convicções religiosas ou filosóficas ou morais, intimidade sexual e, em geral, os que fomentem a discriminação ou afetem a dignidade, a privacidade, a intimidade doméstica e a imagem privada de pessoas ou famílias (RAMINELLI; RODREGHERI, 2016).

No México, a *Ley Federal de Proteccíon de Datos Personales em Posesíon de los Particulares* (LFPDP) foi editada em 2010 e rege o tratamento de dados pessoais desde sua coleta até o armazenamento. Além disso, promove o direito ao acesso, retificação e a solicitação do cancelamento do processamento de dados pelos titulares. Ademais, a Constituição Mexicana confere aos indivíduos direitos de acesso à informação e proteção dos dados pessoais. Já em 2011, Uruguai e Peru instituíram suas leis específicas

acerca do tratamento de dados pessoais denominadas, respectivamente, *Ley de Protección de Datos Personales y Accíon de Habeas Data* e *Ley de Protección de Datos Personales*. A norma uruguaia guarda grandes semelhanças com a argentina e em 2020 passou por uma reforma com a finalidade de se adequar aos ditames da GDPR. Já a lei peruana estrutura a proteção de dados pessoais com foco em proteger os direitos dos indivíduos e garantir o cumprimento das obrigações pelas empresas de processamento de dados, além de promover o acesso transparente às informações públicas. Por último, em terras colombianas, a Lei 1.581/2012 e o Decreto 1.377/2013 regulamentam a proteção de dados pessoais e instituem o *Registro Nacional de Bases de Datos* (RNBD), que tem o objetivo de manter um diretório público das bases de dados pessoais sujeitas a tratamento no país e protege os titulares com o estabelecimento de obrigações para quem coleta e gerencia dados (BRASIL, 2015).

Como se pode notar, há, sobretudo na última década, um forte movimento legislativo para a proteção dos dados das pessoas naturais na América Latina, com forte influência do regulamento europeu sobre o tema. É também evidente que, durante um considerável intervalo de tempo, o Brasil foi o único país integrante do Mercado Comum do Sul (MERCOSUL) que não possuía em seu ordenamento jurídico lei específica de proteção de dados das pessoas naturais, que só veio a ser sancionada em 2018 conforme se verá adiante.

3. DADOS PESSOAIS NO BRASIL: AS NORMATIVAS ANTES DA "LGPD"

No Brasil a proteção de dados pessoais tem como alicerces o fundamento constitucional da dignidade da pessoa humana e os incisos X, XII, XXXIII e LXXII da CRFB/1988, que versam sobre direitos e garantias fundamentais à intimidade, à vida privada, ao sigilo das comunicações e à informação (BRASIL, 1988). Ainda no estudo da seara constitucional, é importante observar o Projeto de Emenda à Constituição (PEC) n° 17 de 2019 que está, ainda, em tramitação no Congresso Nacional e tem a finalidade de incluir expressamente no rol de direitos fundamentais constitucionais a proteção dos dados pessoais, além de fixar a competência privativa da União para legislar sobre a matéria (BRASIL, 2019).

Em que pese ainda não esteja formalmente escrito no texto da CRFB/1988, de acordo com Mendes (2014), a partir de uma análise conjunta da jurisprudência pátria majoritária e dos dispositivos constitucionais citados, é possível afirmar que materialmente o direito fundamental à proteção de dados pessoais é abarcado pelo ordenamento jurídico brasileiro, tese que veio a ser confirmada com o já citado julgamento da ADI 6.387. No âmbito infraconstitucional inicialmente merece

destaque a inclusão do direito à privacidade no Código Civil de 2002 em seu rol de direitos da personalidade, que são, via de regra, intransmissíveis e irrenunciáveis (BRASIL, 2002).

Diante da crescente digitalização, do armazenamento cada vez mais vultoso de dados pessoais e da inexistência de uma lei específica que regulamentasse a proteção de dados pessoais no país, notaram-se, ao longo do tempo, lacunas normativas na tutela de diversas situações que envolviam dados de pessoas naturais em território brasileiro.

A fim de tentar suprimir essas brechas foram incluídas disposições acerca do tema em normas setoriais de caráter federal – como o "Código de Defesa do Consumidor", o "Marco Civil da Internet" e a "Lei de Acesso à Informação"[64] – e outras estaduais e municipais, como as de políticas públicas e mobilidade urbana dispostas em planos diretores municipais participativos. Muitos desses diplomas têm caráter infralegal, como resoluções (*v.g.*, do Conselho Nacional de Autorregulação Publicitária – CONANDA [65]) e portarias do Ministério da Justiça e as resoluções do Banco Central do Brasil (BCB). Nesse momento se faz imperioso ressaltar a possível inconstitucionalidade de algumas dessas normas, em caso de fixação de competência privativa da União para legislar sobre a proteção de dados pessoais como objetiva a PEC 17/2019. Na esfera das normas setoriais, destacamos o Código de Defesa do Consumidor (CDC), que destina uma seção específica para tratar dos bancos de dados e cadastro de consumidores, na qual tutela os direitos dos consumidores à informação, transparência, acessibilidade e visa a coibir que abusos sejam sofridos pela parte hipossuficiente da relação consumerista. Além disso, estabelece a lei obrigações aos órgãos públicos de defesa do consumidor e aos fornecedores de produtos e serviços (BRASIL, 1990).

É assertivo e alinhado à proteção dos dados pessoais o CDC, ao estabelecer a denominada prescrição relativa à cobrança de débitos do consumidor e considerar os serviços de proteção de crédito entidades de caráter público, visto que seria irrazoável e deveras prejudicial permitir o uso perpétuo de informações negativas acerca do consumidor para dificultar o seu acesso ao crédito. Nesse sentido, é pedagógico e atual o voto do então Ministro do Superior Tribunal de Justiça (STJ) Ruy Rosado Aguiar no julgamento do Recurso Especial nº 22.337-8-RS:

> A inserção de dados pessoais do cidadão em bancos de informação tem se constituído em uma das preocupações do Estado moderno, onde o uso da informática e a possibilidade de controle unificado das diversas atividades da pessoa, nas múltiplas situações de vida, permite o conhecimento de sua

[64] Leis Federais n. 8.070, de 11 de setembro de 1990; n. 12.965, de 23 de abril de 2014; e n. 12.527, de 18 de novembro de 2011.
[65] Resolução n. 163, de 4 de abril de 2014.

> conduta pública e privada, até nos mínimos detalhes, podendo chegar à devassa de atos pessoais, invadindo área que deveria ficar restrita à sua intimidade; ao mesmo tempo o cidadão objeto dessa indiscriminada colheita de informações, muitas vezes sequer sabe da existência de tal atividade, ou não dispõe de eficazes meios para conhecer o seu resultado, retificá-lo ou cancelá-lo. E assim como o conjunto dessas informações pode ser usado para fins lícitos, públicos ou privados, na prevenção ou repressão de delitos, ou habilitando o particular a celebrar contratos com pleno conhecimento de causa, também pode servir, ao Estado ou ao particular, para alcançar fins contrários à moral ou ao Direito, como instrumento de perseguição política ou opressão econômica.

É possível notar nas palavras do julgador, proferidas em 1995, a preocupação com situações que são corriqueiras ainda nos dias atuais em que, não raras vezes, consumidores sofrem diversos danos decorrentes de práticas nefastas exercidas por fornecedores por meio do uso abusivo dos dados pessoais obtidos no âmbito da relação consumerista.

Outra norma que merece ser citada neste momento é a Lei Federal nº 12.414, de 9 de junho de 2011, popularmente conhecida como "Lei do Cadastro Positivo", que tem como objetivo regulamentar o povoamento e consulta de bancos de dados com informações acerca do inadimplemento, sejam de pessoas naturais ou jurídicas, com a finalidade de formar um histórico de crédito (BRASIL, 2011). O texto original da Lei do Cadastro Positivo previa a importante garantia da necessidade de consentimento do titular para abertura do cadastro. Entretanto, tal dispositivo foi revogado pela Lei Complementar Federal de nº 166, de 8 de janeiro de 2019, fato que consideramos um retrocesso no âmbito da proteção dos dados pessoais em nosso país. Em que pese a involução, a norma mantém sua relevância na proteção de dados pessoais, visto que foi a pioneira no tratamento de dados sensíveis e reafirmou a "[...] necessidade de controle da atividade de processamento de dados por autoridade administrativa." (MENDES, 2014, p. 147).

Para os propósitos do estudo acerca da proteção de dados pessoais no Brasil, também se faz necessário ressaltar a Lei nº 12.527/2011, conhecida como a "Lei de Acesso à Informação" (LAI), que visa a propiciar mais transparência à Administração Pública, regulamentando o direito fundamental à informação, e guarda estreita relação com o tema em estudo neste artigo, motivo pelo qual será objeto de estudo em tópico específico (BRASIL, 2011). Há ainda um conjunto de diversas outras normas que englobam decretos, portarias, resoluções, entendimentos doutrinários e jurisprudenciais que formam um cenário bastante amplo acerca da proteção de dados pessoais, robusto em alguns setores e frágil noutros. Diante desse contexto e do cenário mundial, se fazia indispensável a instituição de uma lei geral reguladora da

proteção de dados das pessoas naturais no Brasil.

4. "LGPD" NO BRASIL: CONTEXTO, ASPECTOS GERAIS E RELAÇÃO COM A ADMINISTRAÇÃO PÚBLICA

Antes de adentrarmos no estudo das relações entre a Lei Federal 13.709/2018, denominada "Lei Geral de Proteção de Dados Pessoais" (LGPD), e a Administração Pública, para melhor compreensão do tema, se faz necessária a análise do contexto histórico da aprovação da norma e seus aspectos gerais. O pontapé inicial para a discussão da instituição de uma lei geral de proteção de dados pessoais no Brasil foi uma consulta pública, iniciada em dezembro de 2010, elaborada pelo então Ministério da Justiça acerca de um anteprojeto de lei que tinha a finalidade de garantir a proteção de dados pessoais, inclusive na internet. Além disso, visava a adequar o ordenamento pátrio às normas internacionais de proteção de dados pessoais e incluir o país nos debates globais sobre o tema, visto que a ausência de uma lei geral de proteção de dados expunha negativamente o Brasil, além de apresentar um cenário de enorme insegurança jurídica para os seus indivíduos. A consulta teve algumas contribuições, entretanto não ocorreram evoluções relevantes até meados de 2013 (RIELLI, 2019).

Ainda em relação ao anteprojeto de lei, vale a pena destacar que, embora se fundasse em um robusto rol de princípios de proteção de dados pessoais em consonância com as melhores práticas da regulação internacional, ele previa como única hipótese ou base legal de tratamento de dados o consentimento livre, expresso, informado e revogável a qualquer momento pelo titular, com restritas exceções (RAMINELLI; RODEGHERI, 2016).

Em 2013 diante das declarações de Edward Snowden, que já havia trabalhado como administrador de sistemas da *Central Intelligence Agency* (CIA) e terceirizado na *National Security Agency* (NSA), as quais envolviam informações graves e sigilosas sobre diversos governos ao redor do mundo, inclusive o Brasil, intensificou-se ainda mais o movimento global para garantir a proteção dos dados das pessoas naturais. Neste diapasão, em nosso país, foram criados uma Comissão Parlamentar de Inquérito (CPI), com a finalidade de investigar a denúncia da existência de um sistema de espionagem com o objetivo de monitorar dados protegidos pela CRFB/1988, e dois Projetos de Lei voltados para a proteção de dados pessoais. Este movimento impulsionou a aprovação do "Marco Civil da Internet", em 2014, que trouxe consigo um avanço com a instituição, no ambiente *online*, de um microssistema de proteção de dados pessoais, entretanto ainda carregava consigo a limitação de estabelecer o consentimento do titular como única base legal para tratamento de dados pessoais,

característica também notada nos demais Projetos de Lei em tramitação até aquele momento.

Essa singularidade na hipótese de tratamento era considerada uma grande limitação para diversos setores da sociedade visto que, para esses segmentos, se faziam necessárias inclusões de outras hipóteses, com destaque para o legítimo interesse (RIELLI, 2019).

No ano de 2015, em meio a esse amplo debate sobre a proteção de dados pessoais no Brasil, o Ministério da Justiça lançou uma segunda consulta pública, com base em um novo texto de anteprojeto de lei acerca do tema, que teve diversas contribuições de diversificados setores da sociedade, momento em que se notou a necessidade de equilíbrio e harmonização entre o documento e os projetos que já estavam em tramitação no Congresso Nacional, além da inclusão de outras bases legais para tratamento de dados. Desse movimento resultou um robusto anteprojeto apresentado pela então presidenta Dilma Rousseff à Câmara dos Deputados, o qual foi materializado no Projeto de Lei 5.276/2016, que foi alvo de diversos elogios e contou com apoio de diversas entidades da sociedade (RAMINELLI, RODEGUERI, 2016).

Em outubro de 2016 foi criada, sob a relatoria do Deputado Orlando Silva, na Câmara de Deputados, uma Comissão Especial pluripartidária para analisar os projetos de lei acerca da proteção de dados pessoais em tramitação naquela Casa Legislativa. Entretanto, a grande instabilidade política no país e a discussão de um projeto paralelo sobre o tema no Senado Federal retardaram o relatório da Comissão. Todavia, em 2018, a pressão pela aprovação de uma lei geral de proteção de dados no país se intensificou por diversos fatores. Inicialmente, veio à tona o escândalo da *Cambridge Analytica*, que revelou o uso indevido de dados pessoais de diversos indivíduos nas eleições dos Estados Unidos da América (EUA), e em maio daquele ano entrou em vigor o GDPR. Além disso, crescia cada vez mais o interesse do Brasil em ingressar na OCDE e, para isso, necessitava de uma lei de proteção de dados e uma autoridade nacional de proteção de dados. Diante desse cenário, se intensificaram os trâmites e, finalmente, no dia 14 de agosto de 2018 foi sancionada a LGPD (RIELLI, 2019).

Contudo, a LGPD, em seu texto original, previa a entrada em vigor 18 meses após a sua publicação. Entretanto, em 8 de julho de 2019, a Lei 13.853 alterou a *vacatio legis* da norma para 24 meses, a fim de permitir melhor adequação das organizações ao diploma legal. Em 29 de abril de 2020 foi editada a Medida Provisória (MP) 959/2020, que dilatava novamente o prazo de vacância da norma, porém esse trecho da MP não foi convertido em lei. Com isso, à exceção da parte que trata das sanções administrativas, as

quais entrarão em vigor apenas em agosto de 2021, a LGPD entrou em vigor no dia 18 de setembro de 2020 (PEREIRA JUNOR; RAMOS, 2020).

4.1 Aspectos gerais da LGPD

A LGPD, cujas normas gerais são de interesse nacional, dispõe acerca do tratamento de dados pessoais, seja de forma analógica ou digital, por pessoa natural ou por pessoa jurídica de direito público ou privado, com a finalidade de proteger os direitos fundamentais de privacidade, liberdade e o livre desenvolvimento da pessoa natural (BRASIL, 2018). Fortemente inspirada na GDPR, a norma tem caráter essencialmente principiológico e está dividida em dez capítulos que determinam de qual forma os dados pessoais devem ser tratados no Brasil e estabelecem uma série de direitos dos titulares e regras a serem seguidas pelos agentes de tratamento (PINHEIRO, 2020).

Como seus fundamentos, a LGPD traz o respeito à privacidade, a autodeterminação informativa, a liberdade de expressão, de informação, de comunicação e de opinião, a inviolabilidade da honra e da imagem, o desenvolvimento econômico e tecnológico e a inovação, a livre iniciativa, a livre concorrência e a defesa do consumidor e os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais. Observa-se nessa definição dos alicerces do diploma legal grande consonância com os direitos albergados pela CRFB/1988, com destaque para o, reconhecido pelo STF, direito fundamental à proteção de dados pessoais, sem cercear o surgimento de novos modelos econômicos e tecnológicos, visto que "ao mesmo tempo em que objetiva resguardar os dados pessoais não pode desconhecer o andamento para uma nova realidade que se transforma de forma alucinante." (OLIVEIRA, 2020, p. 177).

Na seara principiológica a lei em estudo determina como sustentáculo a observância da boa-fé no tratamento dos dados e consigna diversos princípios dentre os quais merecem destaque os da finalidade, adequação e necessidade. Esta tríade de princípios visa a assegurar que os dados somente serão utilizados para os fins e das formas explicitamente informados ao titular com a proporcionalidade estritamente necessária à consecução dos objetivos. A ênfase se faz necessária porque se nota, por meio da análise dos demais princípios elencados, o objetivo de zelar pelo cumprimento daqueles realçados. Ainda com destaque à boa-fé como princípio base, se faz usual destacar que o seu espectro é amplo e o tratamento deve ser efetuado em conformidade com as expectativas dos titulares e seus direitos e devem ser observados, inclusive por ocasião do uso secundário dos dados pessoais, independentemente da base legal, porque "ausência de consentimento não

equivale a ausência de controle." (BIONI, 2020, p. 227).

Nessa senda das bases legais, que são as hipóteses nas quais é permitido o tratamento de dados das pessoas naturais, a LGPD trouxe um rol de dez enquadramentos, o que pode ser considerado extenso quando comparado ao anteprojeto inicial que previa como única base legal o consentimento do titular. Dentre as hipóteses apresentadas no diploma legal, cabem ser analisadas com maior ênfase o consentimento do titular e o legítimo interesse, que são as mais abrangentes, pois as demais se vinculam a casos concretos específicos.

O consentimento implica na manifestação livre de vícios, inequívoca e informada pela qual o titular admite o tratamento dos seus dados pessoais para uma finalidade específica. Além disso, o indivíduo deve ter acesso a todas as informações atinentes ao tratamento dos dados, incluindo seus métodos, natureza, objetivos, duração, justificativa, finalidades, riscos e benefícios, assim como possuir o direito de, a qualquer momento, recusar ou cessar a operação por meio de procedimento gratuito e facilitado. No âmbito dos dados pessoais sensíveis – que são aqueles que versam sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a organização de caráter religioso, filosófico ou político, referente à saúde ou à vida sexual, dado genético ou biométrico – o consentimento deve ser realizado de forma específica, destacada e para finalidade particularizada. Além disso, em situações que envolvam dados pessoais de crianças e adolescentes, a autorização deve ser dada por pelo menos um dos pais ou pelo responsável legal, exceto quando a coleta se fizer necessária para contatar os pais ou o responsável legal, situação em que os dados não poderão ser armazenados nem repassados a terceiros (MULHOLLAND, 2019).

Já o legítimo interesse, que é a base legal mais flexível entre as elencadas pela LGPD visto que não está atrelado a uma finalidade específica, somente pode ser aplicado no tratamento de dados pessoais para finalidades legítimas, que devem ser aferidas a partir das situações concretas. Exatamente por conta dessa maleabilidade na utilização da hipótese é que o agente de tratamento deve utilizar o mínimo de dados possíveis, adotar medidas para garantir a transparência e pode ser instado, a qualquer momento, pela autoridade nacional protetora de dados a apresentar relatório de impacto à proteção de dados pessoais, observados os segredos comercial e industrial.

Ao decidir utilizar o legítimo interesse como base, o agente responsável pelo tratamento dos dados deve identificar a finalidade do uso, demonstrar a sua real necessidade e, principalmente, sopesar a imprescindibilidade do uso desses dados em face das liberdades fundamentais e da expectativa do titular acerca da operação. Em que pese a maior cautela na utilização dessa

hipótese de tratamento, se faz necessário ressaltar a sua relevância para a manutenção da atualidade da lei em um mundo de constantes inovações tecnológicas e para a viabilidade de tratamento de dados de forma mais célere e eficiente, de modo que não seja necessária a solicitação de consentimento do titular a todo instante (LEONARDI, 2019).

Outro aspecto que deve ser observado é o critério espacial de aplicação da LGPD, visto que vivemos no cenário atual das tecnologias de bancos de dados um expressivo aumento no serviço de *cloud computing*, o qual permite o armazenamento dos dados em qualquer lugar do planeta. Desse modo, a LGPD é assertiva ao determinar a sua aplicação não só para as operações de tratamento efetuadas em território nacional, mas também a todos aqueles dados coletados em território nacional e a qualquer atividade de tratamento que tenha por objetivo a oferta ou o fornecimento de bens ou serviços localizados em solo brasileiro. Nota-se, assim, que pouco importa a localização física do dispositivo que armazena o dado e, com isso, é possível afirmar que a LGPD tem caráter extraterritorial. A norma em análise demonstra, ainda, um grande zelo com a transferência internacional de dados, que somente pode ser efetuada em casos estritos e para países ou organismos internacionais que proporcionem relevante grau de proteção aos dados das pessoas naturais (PINHEIRO, 2020).

Como se pode notar, a LGPD sustenta em diversos pontos do seu texto garantias às pessoas naturais acerca dos seus dados. Não obstante isto, a norma dedicou, ainda, um capítulo próprio assegurando aos indivíduos a titularidade de seus dados pessoais e a garantia aos direitos fundamentais da liberdade, da intimidade e da privacidade, momento em que ressalta os direitos à confirmação da existência de tratamento e do acesso aos seus dados, além de permitir a retificação daqueles que estejam incompletos ou incorretos, solicitar a portabilidade, ser informado em caso de compartilhamento e, com destaque, requerer a eliminação, bloqueio ou anonimização dos dados. Em relação à anonimização, há a previsão expressa na lei de que, sempre que possível, os dados sejam anonimizados, ou seja, manipulem-se, por meio de técnicas razoáveis, de modo que os titulares não possam ser identificados. Entretanto a doutrina demonstra certa descrença acerca da confiabilidade e segurança do processo de anonimização, visto que, a depender da complexidade do meio utilizado, pode ocorrer a reversão do procedimento e a consequente identificação dos titulares dos dados (FRAZÃO, 2019).

A fim de se assegurar o cumprimento dos seus ditames, a LGPD estabelece responsabilização, deveres e sanções aos agentes de tratamento de dados pessoais, sejam eles controladores – a quem competem as decisões referentes aos tratamentos de dados

pessoais – sejam operadores, que são aqueles que realizam o tratamento de dados pessoais em nome do controlador. Para isso, se faz interessante, aqui, vislumbrar a atuação da Administração Pública face à LGPD no exercício do seu poder de polícia (BRASIL, 2018), conforme se aduz abaixo.

4.2 LGPD e Administração Pública brasileira

A Administração Pública pátria tem papel dúplice na LGPD, visto que, além de atuar na fiscalização do cumprimento da lei e aplicação de sanções, no exercício do poder de polícia estatal, por meio da Autoridade Nacional de Proteção de Dados (ANPD), o Poder Público também atua massivamente no tratamento de dados. Tamanha é a expressividade do volume de dados de pessoas naturais tratados pelos órgãos e entidades do Poder Público, que o legislador destinou um capítulo do diploma legal em análise para normatizar o tema (BRASIL, 2018).

É indiscutível que – com ressalva das pessoas jurídicas de direito privado integrantes da Administração Pública que atuam em regime concorrencial – a finalidade do tratamento de dados pelo Poder Público é inteiramente distinta da almejada pelo setor privado, visto que este objetiva essencialmente o lucro econômico. Já no setor público, o tratamento de dados não deriva, via de regra, da voluntariedade do titular, "[...] mas como decorrência das exigências do próprio pacto social: conhecer seus cidadãos é, para o Estado, pré-requisito para o próprio desempenho de suas finalidades públicas." (WIMMER, 2019, p. 127). Cumpre ressaltar que a LGPD não trata com rigor os termos da forma que são conhecidos tradicionalmente na seara administrativista como, por exemplo, Poder Público e Administração Pública. Desse modo, o melhor caminho é interpretar a norma de forma sistemática, com enfoque na atividade efetivamente realizada pelo agente de tratamento no caso específico (WIMMER, 2019).

Nessa perspectiva, nota-se que a LGPD adota critérios distintos no tratamento de dados pelos diversos integrantes do Poder Público. Com base nos ensinamentos de Di Pietro (2019), identifica-se que o diploma legal utiliza o critério objetivo da Administração Pública para delimitar o conceito de Poder Público. Desse modo, preceitua a LGPD, em seu art. 24, que as estatais que atuam em regime concorrencial terão tratamento idêntico ao das pessoas jurídicas de direito privado particulares. Ou, em suas palavras, Di Pietro (2019, p. 77, grifo da autora):

> Em sentido objetivo, a Administração Pública abrange as atividades exercidas pelas pessoas jurídicas, órgãos e agentes incumbidos de atender concretamente às necessidades coletivas; corresponde à função administrativa, atribuída preferencialmente aos órgãos do

> Poder Executivo. Nesse sentido, a Administração Pública abrange o **fomento**, a **polícia administrativa** e o **serviço público**.

A nosso ver foi assertivo o legislador ao adotar o critério objetivo da Administração Pública visto que, em tempos de concessões e parcerias público-privadas, em determinados momentos agentes privados podem assumir atividades típicas do Poder Público, como é o caso dos particulares que exercem por delegação os serviços notariais de registro, e devem gozar das prerrogativas e deveres inerentes aos entes estatais no tratamento de dados.

Além disso, há situações em que pessoas jurídicas de direito privado integrantes da Administração Pública que atuam em regime concorrencial – e, em tese, devem se submeter ao mesmo regime imposto aos particulares – atuam estritamente em prol do interesse público, como é o caso da Empresa Brasileira de Correios e Telégrafos, que detém, com amparo constitucional, o monopólio dos serviços postais, entretanto no ramo de entrega de encomendas atua num ramo econômico livre e de caráter eminentemente privado. Nota-se, nesses casos, um regime híbrido e, diante disso, deve ser aplicada a norma de acordo com a finalidade exercida pela entidade no ato concreto do tratamento de dados.

Com o fim de salvaguardar a execução das atividades exercidas na acepção objetiva da Administração, a LGPD estabelece expressamente uma base legal específica a fim de permitir, aos entes que exercem atividades nesse espectro, o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em atos normativos ou respaldadas em contratos, convênios ou instrumentos congêneres.

Apesar da unicidade de hipótese explícita no texto da norma, Wimmer (2019) afirma que, a partir de uma análise sistêmica, é possível encontrar na lei outra base legal direcionada à Administração Pública: a do tratamento de dados pessoais na execução de competências ou atribuições legais do serviço público. Além disso, a eminente autora aponta a incerteza acerca da possibilidade de o Poder Público invocar as demais bases legais, momento em que ressalta a dinamização cada vez maior das relações entre os entes da Administração Pública e os cidadãos, baseadas cada vez mais no uso de tecnologias, o que pode ensejar o tratamento de dados com lastro em outras hipóteses e, diante disso, assevera a grande necessidade de atuação da ANPD na regulamentação e esclarecimentos acerca dessas lacunas.

Ainda na seara da incidência da LGPD no exercício das atividades pelo Poder Público, faz-se necessário ressaltar a não incidência da norma nos tratamentos realizados para fins exclusivos de segurança pública, defesa nacional, segurança do Estado e em atividades de investigação e repressão de infrações penais. Entretanto, é importante

ressaltar que essa inaplicabilidade não consiste numa carta branca para o tratamento de dados de forma arbitrária pelo Poder Público nessas situações, visto que a própria LGPD preceitua que o tratamento nos casos citados deverá ser realizado apenas em casos estritamente necessários, em atendimento ao interesse público e, para além, se regerá por legislação específica e observará os princípios gerais de proteção de dados, os direitos do titular e o devido processo legal.

Nesse diapasão, em novembro de 2020, foi entregue à Câmara de Deputados um anteprojeto de lei que visa a regulamentar o tratamento de dados pessoais nas atividades de segurança pública e persecução criminal (BARRETO; MARQUES; PAULO NETO, 2020). Ante o exposto, resta clarividente a responsabilidade civil do Poder Público por danos causados no tratamento de dados pessoais. Entretanto, embora a LGPD preveja a responsabilização e ressarcimento de danos no caso de tratamento irregular, não há, na norma, diretriz específica de responsabilização civil das pessoas que atuam no sentido objetivo da Administração Pública. Desse modo, resta a dúvida acerca da objetividade ou subjetividade da responsabilidade na hipótese de tratamento irregular por entes governamentais. De acordo Alvim e Pereira (2020), esta é mais uma situação que carece de regulamentação pela ANPD, porém, enquanto não ocorre a definição pela entidade, o caminho mais seguro a ser seguido é o da responsabilização objetiva aos integrantes da Administração Pública.

A fim de que sejam evitadas irregularidades no tratamento de dados, a LGPD possibilita a criação de regras de boas práticas e governança pelos agentes de tratamentos de dados pessoais com o estabelecimento de procedimentos, normas de segurança, padrões técnicos, ações educativas e outros mecanismos relacionados ao tratamento de dados pessoais. Tal permissão decorre dos desafios e novidades que a norma impõe aos atores no ato da manipulação dos dados das pessoas naturais. Na lição de Wimmer (2019), para o setor público o desafio é ainda maior, visto que a transformação digital no ramo está ocorrendo paralelamente a essa necessidade de adequação à LGPD. Com isso, faz-se mister o exercício do princípio boa administração pública que é:

> Aquele direito fundamental à administração pública eficiente e eficaz, proporcional cumpridora dos seus deveres, com transparência, sustentabilidade, motivação proporcional, imparcialidade e respeito à moralidade, à participação social e à plena responsabilidade por suas condutas comissivas e omissivas. (FREITAS, 2014, p. 21).

Nessa perspectiva, para a consolidação de uma boa Administração Pública, que zele pelo tratamento dos dados pessoais, é impreterível a existência de uma autoridade de proteção de dados independente e com condições para cumprir os

mandamentos a ela atribuídos pela LGPD. Mas quem seria ela?

4.2.1 Autoridade Nacional de Proteção de Dados: um órgão regulador?

A ANPD é, atualmente, um órgão da Administração Pública Federal integrante da Presidência da República, criado pela Lei 13.853/2019, que a assegura autonomia técnica e decisória, institui a sua composição e lhe atribui a finalidade de zelar, estabelecer e fiscalizar o cumprimento da LGPD em todo o território nacional (BRASIL, 2019). A ANPD possui um extenso rol de competências atribuídas pela LGPD, dentre as quais se destacam a fiscalização e aplicação de sanções em caso de tratamento de dados realizado em descumprimento com a legislação, elaboração de diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade, promoção e elaboração de estudos sobre as práticas nacionais e internacionais de proteção de dados pessoais e privacidade, estímulo à adoção de padrões de serviços e produtos que facilitem o exercício de controle dos titulares sobre seus dados pessoais e a conscientização da população acerca do conhecimento das normas e das políticas públicas sobre a proteção de dados pessoais e das medidas de segurança (BRASIL, 2019).

É indiscutível, na dinâmica global contemporânea, a relevância de uma entidade regulamentadora do tratamento de dados pessoais. Entretanto, no Brasil, o caminho para a instituição da ANPD foi tortuoso e, mesmo após a sua criação, persistem pontos conflitantes acerca da autoridade. A problemática pode ser identificada desde o momento do envio do projeto de lei de proteção de dados pelo Poder Executivo, que posteriormente veio a resultar na LGPD e não previa a criação de uma autoridade de proteção de dados. Diante disso, no decorrer da discussão no Congresso Nacional, houve a inclusão no texto da previsão do ente fiscalizador que, todavia, foi vetado pelo então Presidente da República, Michel Temer, sob o argumento de que consistia em um vício de iniciativa porquanto a previsão fora incluída pelo Poder Legislativo e tal competência seria privativa do Poder Executivo (VALENTIM, 2020).

O veto à criação da ANPD gerou, naquele momento, um enorme problema, visto que havia, mesmo que com expressiva *vacatio legis*, uma lei de proteção de dados pessoais no ordenamento jurídico, entretanto não existia uma entidade para zelar pelo cumprimento desta norma. Ciente de tal problema e diante da reconhecida importância de se ter uma autoridade de controle para o cumprimento da LGPD e o bom funcionamento do sistema nacional de proteção de dados, o próprio Presidente Michel Temer, logo em seguida, editou a MP nº 869/2018, que posteriormente veio a ser convertida na Lei nº 13.853/2019, estabelecendo a criação da ANPD.

Contudo, a ANPD foi concebida com características diferentes daquelas que lhe eram atribuídas pela redação original da LGPD. Enquanto no texto original a ANPD era integrante da Administração Pública Indireta, possuindo natureza jurídica de autarquia em regime especial, a autoridade foi criada transitoriamente como órgão vinculado à Presidência da República, com a possibilidade de no prazo de dois anos a partir da entrada em vigor da sua estrutura regimental (que ocorreu em 15 de outubro de 2020) a critério do Poder Executivo, ser transformada em autarquia em regime especial. Essa mutação da natureza jurídica implica significativas diferenças e gerou dúvidas, sobretudo acerca da autonomia da autoridade, que se tornaram ainda mais acentuadas diante dos vetos do Presidente Jair Bolsonaro a alguns dispositivos da Lei nº 13.853, de 8 de julho de 2019, que reforçavam a autonomia da ANPD, os quais foram apreciados e, felizmente, rejeitados pelo Congresso Nacional (FERRAZ, 2020).

É expressiva a diferença entre um órgão e uma autarquia em regime especial, categoria em que se enquadram todas as agências reguladoras federais em funcionamento no Brasil. Os órgãos são desprovidos de personalidade jurídica, visto que consistem apenas em parte integrante de uma pessoa jurídica e, diante disso, há uma inerente subordinação hierárquica, além da ausência de um orçamento próprio, fato que dificulta, por exemplo, a organização de um quadro próprio de servidores. Já as autarquias em regime especial têm personalidade jurídica própria, são dotadas de autonomia gerencial, orçamentária e patrimonial, além de disporem de quadro próprio de servidores e não serem hierarquicamente subordinadas à Administração Pública Direta, possuindo, assim, uma maior margem de liberdade ou discricionariedade técnica (DI PIETRO, 2019). Nesse diapasão, mesmo com a disposição expressa, na LGPD, da autonomia técnica e decisória da ANPD, a subordinação financeira da autoridade implica riscos à sua independência que se tornam ainda mais iminentes diante da sujeição do próprio setor público ao regramento da norma (FERRAZ, 2020).

Em 26 de outubro de 2020, a OCDE publicou um extenso relatório acerca da transformação digital brasileira, no qual recomendou fortemente a independência da ANPD e citou expressamente a necessidade de revisão do modelo de estruturação da entidade e "a esse respeito a conversão da ANPD em um modelo autárquico é um dos pilares para a digitalização da economia brasileira, ao mesmo tempo que é um trunfo para que o estado brasileiro efetive seu ingresso na OCDE." (BIONI; PIGATTO, 2020).

Diante do exposto, a nosso ver e a fim de garantir a autonomia necessária para o exercício do seu extenso rol de atribuições, o melhor modelo para a ANPD é o de autarquia em regime especial, assim como ocorre com

as agências reguladoras federais, visto que a proteção dos dados das pessoas naturais é tema sensível e de relevância tão expressiva quanto o tratado por aquelas entidades.

5. A "LGPD" E A "LAI": ANTINOMIA OU COMPLEMENTARIDADE?

A novidade da Lei Geral de Proteção de Dados gerou, em vários setores da sociedade, discussões acerca da temática da proteção de dados das pessoas naturais no Brasil. Um dos principais debates versa sobre uma possível antinomia entre a LGPD e a LAI, norma que tem como finalidade regular o acesso às informações de interesse público constantes dos bancos de dados mantidos por órgãos e entidades da Administração Pública e entidades privadas sem fins lucrativos que recebam recursos públicos para a realização de ações de interesse da coletividade (BRASIL, 2011).

Incialmente se faz fundamental ressaltar que a LAI é um dos principais instrumentos de concretização da transparência pública – a qual decorre do direito fundamental à informação e do princípio da publicidade da Administração Pública – que é basilar para a subsistência do Estado Democrático de Direito e exerce um papel fundamental para o interesse público e, para além disso, exerce um duplo papel, visto que promove o controle da sociedade sobre o Poder Público e ampara o acesso às informações por ele armazenadas aos indivíduos (CANHADAS, 2020).

Nessa perspectiva, nota-se o relevante papel exercido pela LAI na organização e difusão da transparência pública, colocando em prática os princípios do interesse coletivo, do bem comum e da supremacia do interesse público, franqueando aos cidadãos o acesso a dados detidos pela Administração Pública, suprindo anseios da sociedade acerca da informação. Porém, cumpre ressaltar que o acesso à informação concedido pela norma não é ilimitado visto que, não obstante o fato de a norma em análise tratar como regra a publicidade e o sigilo como exceção, a LAI dedica um capítulo para versar sobre restrições de acesso à informação, em que prevê hipóteses de classificação e sigilo além de ressaltar a necessidade de respeito à intimidade, honra e imagem das pessoas, vida privada e às liberdades e garantias individuais no tratamento das informações pessoais (BRASIL, 2011).

Em que pese ser possível a negativa do acesso à informação – a qual sempre que ocorrer deve ser expressamente motivada –, a recusa só é justificável em situações de extrema sensibilidade como, por exemplo, em casos de ameaça à soberania nacional ou à vida da população. Entretanto, a restrição ao acesso em nenhuma hipótese será eterna, visto que a LAI prevê prazos máximos para a limitação, além de estabelecer um limitado rol de autoridades que podem estabelecer o sigilo.

A importância de um reduzido número de servidores aptos a estabelecer restrição foi enfatizada no início de 2019 quando o então Presidente em exercício Hamilton Mourão editou o Decreto Federal 9.690, de 23 de janeiro de 2019, que ampliava expressivamente o rol de autoridades permitidas a impor graus de sigilo secreto e ultrassecreto a documentos públicos e, com isso, transformaria a "Lei de Transparência" numa verdadeira norma de opacidade pública. Felizmente, após forte pressão da mídia e da classe política, o decreto foi revogado pelo Presidente da República em atividade (ANGÉLICO, 2019).

Ademais nota-se, ao analisar o texto da LAI, que para além da especial preocupação com as informações pessoais, termo a que atribui conceito similar ao de dado pessoal na LGPD, houve também a responsabilização dos agentes nos casos de tratamento indevido e o viés, com raras exceções, do consentimento do titular ou previsão legal para divulgação de informações. Nessa perspectiva constata-se que o conflito entre LGPD e LAI é apenas aparente, visto que ambas as normas visam a garantir a concretização dos direitos e garantias fundamentais outorgados aos indivíduos pela CRFB/1988 e, com isso, devem ser interpretadas e aplicadas de forma harmônica com a finalidade de conferir aos cidadãos maior segurança acerca dos seus dados. Para isso, a LGPD traz mecanismos que reforçam a necessidade de zelo no tratamento dos dados das pessoas naturais, que deve ser efetuado de forma segura e estritamente para a finalidade à qual o dado foi coletado e dispõe, inclusive, acerca da possibilidade da solicitação pela ANPD de relatório de impacto da operação, que deve conter descrição dos tipos de dados, metodologia de coleta e mecanismos de segurança adotados.

Ademais, a LGPD traz ao ordenamento jurídico uma nova visão acerca da distinção entre dados públicos e sigilosos, visto que, para a norma em análise, os dados das pessoas naturais devem ser protegidos independentemente do seu grau de sigilo. Desse modo, se concebe ao indivíduo maior transparência no tratamento dos seus dados, além da aplicação de técnicas de anonimização dos dados sempre que possível e esmero ainda maior nas operações que envolvam dados sensíveis. Diante do exposto, a partir de uma análise conjunta das normas sob o prisma constitucional, verifica-se que tanto a LAI quanto a LGPD são normas que versam acerca do tratamento de dados pessoais e são alicerceadas no tripé confidencialidade, integridade e disponibilidade, com o fim de garantir o acesso à informação sem negligenciar a proteção dos dados pessoais.

CONSIDERAÇÕES FINAIS

O desenvolvimento do presente trabalho evidenciou a importância da tutela

jurídica aos dados das pessoas naturais diante do exponencial e contínuo desenvolvimento das tecnologias da informação e comunicação e poderosos métodos de armazenamento e análise de dados. Verificou-se, ainda, a evolução de proteção de dados em todo o mundo e as influências e histórico legislativo até que, finalmente, fosse sancionada a Lei Geral de Proteção de Dados no Brasil, sem prejuízo das normas isoladas, já editadas até então, que versam sobre o mesmo tema. Diante da novidade da norma analisaram-se seus aspectos gerais e, de forma mais aprofundada, a sua relação com a Administração Pública. Com isso, foi possível notar o preponderante papel que o Poder Público exerce na proteção dos dados pessoais, não só pelo fato de deter a maior base de dados acerca das pessoas naturais no Brasil, mas também pelo seu dever de atuar como guardião da norma, velando pelo seu pleno cumprimento.

Nessa seara, é preocupante o enquadramento da ANPD como órgão público vinculado diretamente à Presidência da República, visto que este modelo limita a autonomia financeira, gerencial e fiscalizatória da autoridade, fato que pode causar o fracasso de todo o esforço em torno da proteção de dados das pessoas naturais no país e, diante disso, deixar brechas para tratamentos indevidos dos quais podem decorrer sequelas graves em toda a sociedade brasileira. Em tempos de pandemia, essa situação é ainda mais inquietante, visto que podem ser alegadas hipóteses legais de tratamento relacionadas à saúde para utilização dos dados com finalidade diversa. Diante disso, a nosso ver, o melhor caminho é a transformação da ANPD, pelo Congresso Nacional, em autarquia em regime especial. Enquanto isto não acontece, o Poder Judiciário deve se manter alerta e firme na defesa dos indivíduos, assim como bem fez no julgamento da ADI (Ação Declaratória de Inconstitucionalidade) 6.387/2019 – manifesta no Supremo Tribunal Federal.

No tocante ao conflito entre a LAI e LGPD, entendemos que, em verdade, as normas se complementam no interesse constitucional de tutelar os direitos à transparência e proteção dos dados pessoais dos cidadãos e, para isso, devem ser interpretadas de forma harmônica e sistemática sob a égide da CFRB/1988. Assim, cumpre ressaltar que a sociedade civil e as instituições devem permanecer sempre vigilantes para que a LGPD seja utilizada para o fim a que se destina, que é a proteção dos dados das pessoas naturais, e jamais para fins políticos ou como ferramenta ilegal para omitir dos cidadãos informações às quais têm pleno direito de acesso – tendo em vista os tempos que se encontram atualmente e a (in)disposição do Poder Público na completa proteção dos dados dos cidadãos brasileiros a quem quer que seja.

REFERÊNCIAS

ALVIM, R. S; PEREIRA, F. R. U. A responsabilidade civil do Estado por danos decorrentes do tratamento de dados pessoais: um estudo de caso. In: MARTINS, R. M. (Coord.); DAL POZZO, A. N. (Coord). **LGPD e Administração Pública: uma análise ampla dos impactos**. São Paulo: Thomson Reuters Brasil. 2020. p. 808-847.

ANGÉLICO, FABIANO. **Decreto contraria espírito da Lei de Acesso à Informação**. 25 de janeiro de 2019. Disponível em: <https://complemento.veja.abril.com.br/pagina-aberta/decreto-contraria-espirito-da-lei-de-acesso-a-informacao.html>. Acesso em: 12 abr. 2021.

ARAÚJO, Alexandra Maria Rodrigues; OLIVEIRA, José Sebastião de. A transferência de dados pessoais para países terceiros acompanhada de uma decisão de adequação no Direito da União Europeia. In: CONPEDI/2014/UFPB, XXIII, Encontro, 2014. **Anais**... João Pessoa: FUNJAB, 2014. Disponível em: <http://www.publicadireito.com.br/publicacao/ufpb/livro.php?gt=252>. Acesso em: 18 mar. 2021.

BARRETO, Pablo Coutinho; MARQUES, Paulo Rubens Carvalho; PAULO NETO, Octávio Celso Gondim. **O anteprojeto da 'LGPD penal' e a (in) segurança pública e (não) persecução penal**. 9 de dezembro de 2020. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/o-anteprojeto-da-lgpd-penal-e-a-in-seguranca-publica-e-nao-persecucao-penal-09122020>. Acesso em 10 abr. 2021.

BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. 2 ed. Rio de Janeiro: Forense, 2020.

BIONI, Bruno Ricardo; PIGATTO, Jaqueline Trevisan. **A Autoridade Nacional de Proteção de Dados e o possível ingresso do Brasil na OCDE**. 4 de novembro de 2020. Disponível em: < https://www.observatorioprivacidade.com.br/2020/11/04/a-autoridade-nacional-de-protecao-de-dados-e-o-possivel-ingresso-do-brasil-na-ocde/>. Acesso em: 1 mar. 2021.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituição.htm>. Acesso em: 31 mar. 2021.

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.** Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm>. Acesso em: 28 out. 2020.

BRASIL. Ministério da Justiça. **Proteção de dados pessoais pelo mundo**. 17 de abril de 2015. Disponível em: <http://pensando.mj.gov.br/dadospessoais/2015/04/protecao-de-dados-pessoais-pelo-mundo/>. Acesso em: 5 abr. 2021.

BRASIL. Senado Federal. **Proposta de Emenda à Constituição n° 17, de 2019**. Acrescenta o inciso XII-A, ao art. 5º, e o inciso XXX, ao art. 22, da Constituição Federal para incluir a proteção de dados pessoais entre os direitos fundamentais do cidadão e fixar a competência privativa da União para legislar sobre a matéria. Brasília: Senado Federal, 2019. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/135594>. Acesso em: 10 abr. 2021.

BRASIL. Superior Tribunal de Justiça. **REsp nº 22.337/RS**. 4ª Turma. Relator: Ministro Ruy Rosado de Aguiar. Julgado em 13/02/1995. DJU, p. 6119, mar. 1995. Disponível em: <https://stj.jusbrasil.com.br/jurisprudencia/20254988/recurso-especial-resp-22337-rs-1992-0011446-6/inteiro-teor-104873141>. Acesso

em: 22. mar. 2021.

BRASIL. Supremo Tribunal Federal. **ADI nº 6.387/DF**. Relatora: Ministra Rosa Weber. Julgado em 07/05/2020. DJE nº 270. Disponível em: <http://portal.stf.jus.br/processos/detalhe.asp?incidente=5895165>. Acesso em: 24. mar. 2021.

CAMARGO, Winícios Waldemar dos Santos; TAGLIAFERRO, Eduardo. A influência dos vazamentos de dados pessoais para a construção da legislação atual. **Revista Científica Intr@ciência**, São Paulo, v. 1, n. 20, p. 1-13, dez. 2020. Disponível em: < https://uniesp.edu.br/sites/_biblioteca/revistas/20201125003402.pdf>. Acesso em: 2 abr. 2021.

CARVALHO, Lucas Borges de. 16 de dezembro de 2020. **A LGPD e o acesso a informação pública: dado pessoal é dado sigiloso?** Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/lgpd-informacao-publica-16122020>. Acesso em: 15 mar. 2021.

CARVALHO, Solano de. As sanções da LGPD e o Inferno de Dante. **Revista do Advogado**, São Paulo, v. 39, n. 144, p. 220-225, nov. 2019. Disponível em: <https://aplicacao.aasp.org.br/aasp/servicos/revista_advogado/paginaveis/144/index.html?_ga=2.210407445.1099744738.1617372899-714799726.1617056820>. Acesso em: 28 fev. 2021

CASTRO, Catarina Sarmento e. O direito à autodeterminação informativa e os novos desafios gerados pelo direito à liberdade e à segurança no pós 11 de Setembro. In: VIII Congresso Ibero-Americano de Direito Constitucional. 2003, Sevilha. Disponível em: <https://egov.ufsc.br/portal/sites/default/files/anexos/5544-5536-1-PB.pdf>. Acesso em: 13. mar. 2021.

DALESE, Pedro. **Aspectos gerais sobre o PL de proteção de informações pessoais da China**. 30 de março de 2021. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/protecao-dados-pessoais-china-20112020>. Acesso em: 2 abr. 2021.

DI PIETRO, Maria Sylvia Zanella. **Direito Administrativo**. 32 ed. Rio de Janeiro: Forense, 2019.

DONEDA, Danilo. **Da privacidade dos dados pessoais**. Rio de Janeiro: Editora Renovar, 2006.

FERRAZ, P. C. Autoridade Nacional de Proteção de Dados (ANPD): apontamentos sobre sua natureza e regime jurídico. In: MARTINS, R. M. (Coord.); DAL POZZO, A. N. (Coord). **LGPD e Administração Pública: uma análise ampla dos impactos**. São Paulo: Thomson Reuters Brasil. 2020. p. 621-643.

FRAZÃO, Ana. Direitos básicos dos titulares de dados pessoais. **Revista do Advogado**, São Paulo, v. 39, n. 144, p. 33-46, nov. 2019. Disponível em: <https://aplicacao.aasp.org.br/aasp/servicos/revista_advogado/paginaveis/144/index.html?_ga=2.210407445.1099744738.1617372899-714799726.1617056820>. Acesso em: 28 fev. 2021.

FREITAS, Juarez. **Direito fundamental à boa administração pública.** 3. ed. São Paulo: Malheiros, 2014.

HALPERT, Jim. **US: Virginia passes comprehensive consumer data protection law**. 18 de março de 2021. Disponível em: <https://blogs.dlapiper.com/privacymatters/us-virginia-passes-comprehensive-consumer-data-protection-law/>. Acesso em: 24. mar. 2021.

LEONARDI, Marcel. Legítimo interesse. **Revista do Advogado**, São Paulo, v. 39, n. 144, p. 67-73, nov. 2019. Disponível em: <https://aplicacao.aasp.org.br/aasp/servicos/revista_advogado/paginaveis/144/index.html?_ga=2.210407445.1099744738.1617372899-714799726.1617056820>. Acesso em: 28 fev. 2021.

LISBOA, Roberto Senise. Boa-fé e confiança

na Lei Geral de Proteção de Dados brasileira. **Revista do Advogado**, São Paulo, v. 39, n. 144, p. 74-79, nov. 2019. Disponível em: <https://aplicacao.aasp.org.br/aasp/servicos/revista_advogado/paginaveis/144/index.html?_ga=2.210407445.1099744738.1617372899-714799726.1617056820>. Acesso em: 28 fev. 2021.

MACHADO, Joana de Moraes Souza. **A tutela da privacidade na sociedade da informação**: a proteção de dados pessoais no Brasil. Porto Alegre: Editora Fi, 2018.

MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: Linhas gerais de um novo direito fundamental. São Paulo: Editora Saraiva, 2014.

MOLINARI, Lia Hebe; SEBASTIAN, Maria Alejandra; VÁZQUEZ, Nadia Estefania. Caso de estudio sobre GDPR aplicado em Sistemas de Gestión Académica. In: XXIV Congreso Argentino de Ciencias de la Computación. 2018, Tandil. Disponível em: <http://sedici.unlp.edu.ar/bitstream/handle/10915/73652/Documento_completo.pdf-PDFA.pdf?sequence=1&isAllowed=y>. Acesso em: 23. mar. 2021.

MORAES, Alexandre de. **Direito Constitucional**. 36 ed. São Paulo: Atlas, 2020.

MULHOLLAND, Caitlin. Dados pessoais sensíveis e consentimento na Lei Geral de Proteção de Dados Pessoais. **Revista do Advogado**, São Paulo, v. 39, n. 144, p. 47-53, nov. 2019. Disponível em: <https://aplicacao.aasp.org.br/aasp/servicos/revista_advogado/paginaveis/144/index.html?_ga=2.210407445.1099744738.1617372899-714799726.1617056820>. Acesso em: 28 fev. 2021.

OLIVEIRA, R. F. Os fundamentos da Lei de Proteção de Dados Pessoais. In: MARTINS, R. M. (Coord.); DAL POZZO, A. N. (Coord). **LGPD e Administração Pública: uma análise ampla dos impactos**. São Paulo: Thomson Reuters Brasil. 2020. p. 167-178.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **Declaração Universal dos Direitos Humanos**. Rio de Janeiro: UNIC, 2009 [1948]. Disponível em: <http://www.dudh.org.br/wp-content/uploads/2014/12/dudh.pdf> Acesso em: 27 abr. 2021.

PEREIRA JUNIOR, Ademir Antônio; RAMOS, Luiz Felipe Rosa. **Lei Geral de Proteção de Dados, um ano de formação**. 7 de dezembro de 2020. Disponível em <https://www.conjur.com.br/2020-dez-07/direito-digitallgpd-ano-formacao>. Acesso em: 6 abr. 2021.

PINHEIRO, Patricia Peck. **Proteção de Dados Pessoais**: comentários à Lei n. 13.709/2018 (LGPD). 2 ed. São Paulo: Editora Saraiva, 2020.

QUEIROZ, Rafael Mafei Rabelo. Direito à privacidade e proteção de dados pessoais: aproximações e distinções. **Revista do Advogado**, São Paulo, v. 39, n. 144, p. 74-79, nov. 2019. Disponível em: < https://aplicacao.aasp.org.br/aasp/servicos/revista_advogado/paginaveis/144/index.html?_ga=2.210407445.1099744738.1617372899-714799726.1617056820>. Acesso em: 28 fev. 2021.

RAMINELLI, Francieli Puntel; RODEGHERI, Letícia Bodanese. A proteção de dados pessoais no Brasil: análise de decisões proferidas pelo Supremo Tribunal Federal. **Cadernos do Programa de Pós-graduação**, Porto Alegre, v. 2, n. 2, p.89-119, 2016. Disponível em: <https://seer.ufrgs.br/ppgdir/article/download/61960/39936>. Acesso em: 31. mar. 2021.

REIS, Rafael Almeida Oliveira. **A nova administração de Joe Biden e o rumo da privacidade nos Estados Unidos**. 30 de janeiro de 2021. Disponível em: <https://blog.bluetax.com.br/profiles/blogs/a-nova-administracao-de-joe-biden-e-o-rumo-da-privacidade-nos-est>. Acesso em 24. mar. 2021.

RIELLI, Mariana Marques. O processo de construção e aprovação da Lei Geral de Dados

Pessoais: bases legais para tratamento em um debate multissetorial. **Revista do Advogado**, São Paulo, v. 39, n. 144, p. 7-14, nov. 2019. Disponível em: <https://aplicacao.aasp.org.br/aasp/servicos/revista_advogado/paginaveis/144/index.html?_ga=2.210407445.1099744738.1617372899-714799726.1617056820>. Acesso em: 28 fev. 2021.

SILVA, José Afonso da. **Curso de Direito Constitucional Positivo**. 25 ed. São Paulo: Malheiros Editores, 2005.

VALENTIM, R. M. O contexto brasileiro da proteção de dados pessoais e as características da autoridade nacional de proteção de dados. In: MARTINS, R. M. (Coord.); DAL POZZO, A. N. (Coord). **LGPD e Administração Pública: uma análise ampla dos impactos**. São Paulo: Thomson Reuters Brasil. 2020. p. 603-620.

WIMMER, Miriam. Proteção de dados pessoais no Poder Público: incidência, bases legais e especificidades. **Revista do Advogado**, São Paulo, v. 39, n. 144, p. 126-133, nov. 2019. Disponível em: <https://aplicacao.aasp.org.br/aasp/servicos/revista_advogado/paginaveis/144/index.html?_ga=2.210407445.1099744738.1617372899-714799726.1617056820>. Acesso em: 28 fev. 2021.