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 |

CHALLENGES AND PERSPECTIVES FOR THE PROTECTION OF SENSITIVE PERSONAL DATA IN POWER OF THE PUBLIC ADMINISTRATION: BETWEEN THE PUBLIC DUTY TO INFORM AND THE CITIZEN'S RIGHT TO BE PROTECTED

MARIANA ROCHA DE FLÔRES
ROSANE LEAL DA SILVA

RESUMO | A Administração Pública compreende como princípios norteadores a transparência e a publicidade, conforme previsão da Lei n.° 12.527/2011, porém o seu âmbito de atuação está diretamente ligado a dados pessoais sensíveis que não devem ser publicizados. Por conta disso, questiona-se se a disciplina dos dados pessoais sensíveis, recentemente regulada pela Lei n.º 13.709/2018, se mostra adequada e suficiente quando o tratamento for feito pelo Poder Público. Na busca de enfrentar o tema, foi desenvolvida análise da evolução histórica da proteção de dados pessoais, até se chegar nas possíveis mudanças encontradas na nova Lei. No estudo realizado, conclui-se que a Lei n.º 13.709/18 adentra o ordenamento jurídico com uma importante função social. Todavia, não se encontra nela amparo suficiente em relação aos dados pessoais sensíveis em poder da Administração Pública, visto que sua proteção abrange muito mais a esfera privada.

PALAVRAS-CHAVE | Administração Pública. Dados Pessoais Sensíveis. Lei n.º 13.709/18. Proteção de Dados.

ABSTRACT *| Public Administration understands transparency and publicity as guiding principles, as provided by Law n. 12.527/2011. However, its sphere of action is directly linked to sensitive personal data that should not be published. Because of that, it is questioned whether the use of these data, recently regulated by Law n. 13.709/2018, is adequate and sufficient when it is done by the Public Authority. In an attempt to tackle the issue, an analysis of the historical evolution of the protection of personal data was carried out until reaching the possible changes found in the new Law. In the study, it is concluded that Law n. 13.709/18 enters the legal system with an important social function, but support has not been sufficiently found in relation to sensitive personal data held by the Public Administration. In spite of that, the private sector has a greater cover of data protection.*

***KEYWORDS* |** *Public Administration. Sensitive Personal Data. Law n.13.709/18. Data Protection.*

1. INTRODUÇÃO

No Brasil, a proteção de dados pessoais tem como uma de suas características marcantes a criação tardia de normas adequadas em relação a outros países. Isso ocorre porque, no Brasil, as primeiras demonstrações desses mecanismos de proteção se deram através do *habeas data* (art. 5º, inc. LXXII, Constituição Federal) e do banco de dados dos consumidores, previsto no Código de Defesa do Consumidor, enquanto que, em outros países, como Alemanha e Suíça, já havia regulamentações específicas sobre o tema – apesar de algumas não terem contemplado o tratamento adequado.

Com a evolução da tecnologia, sobretudo aplicativos e *sites* de redes sociais que permitem a interação de forma rápida e incontrolável, surge a necessidade de reforçar, cada vez mais, os mecanismos de proteção de dados pessoais, tendo em vista que a sociedade, na conjuntura atual, baseia-se nas tecnologias, o que gera exposição constante.

Práticas habituais do cotidiano, como participar de uma rede social, fazer um cadastro em um *site* de compras ou em plataformas de currículos e até mesmo para participar de programas governamentais, como o Exame Nacional do Ensino Médio (ENEM), têm como exigência o fornecimento de informações pessoais. No entanto, muitas vezes, as pessoas não mensuram a extensão do problema que a disponibilização dessas informações pode gerar, de modo que parecem ignorar as inúmeras possibilidades desses dados não serem suficientemente protegidos, podendo ser utilizados de forma equivocada.

Existem diferentes tipos de dados utilizados nesses cadastros e que poderiam ser objeto de atenção, mas, para melhor delimitar o tema de análise, o foco desta pesquisa é tratar dos dados pessoais sensíveis em poder da Administração Pública, que envolvem questões de cunho totalmente íntimo e individual. Esses dados tratam de aspectos raciais, étnicos, ideológicos e de orientação sexual, além de informações confidenciais referentes à saúde do indivíduo, por exemplo. A disponibilização indevida desses dados pode servir

como instrumento para o cometimento de discriminação, intolerância e constrangimento de seu titular.

Devido à falta de regulamentação específica para tratar de dados sensíveis, ao que se soma a atuação da Administração Pública, que é detentora de deveres de transparência e publicidade, muitas são as dificuldades no tratamento e controle desses dados, o que suscita o seguinte problema de pesquisa: Considerando a produção doutrinária existente sobre o tema e os princípios como igualdade, não discriminação e promoção da dignidade humana, pode-se afirmar que a disciplina dos dados pessoais sensíveis, recentemente regulada pela Lei n.º 13.709/2018, mostra-se adequada e suficiente quando o tratamento for feito pelo Poder Público?

No intuito de responder a essa questão, a pesquisa foi elaborada valendo-se do método de abordagem dedutivo, visto que parte da análise geral dos conceitos e marcos temporais que envolvem a proteção de dados pessoais até chegar aos seus desdobramentos específicos, referentes aos dados sensíveis em poder da Administração Pública, o que é feito à luz da nova Lei n.º 13.709/18.

Aliado ao método de abordagem dedutivo, foram empregados os métodos de procedimento histórico e comparativo, considerando que essa investigação abrange a evolução histórica da proteção de dados e demonstra como era regida essa proteção no âmbito da Administração Pública antes da vigência da Lei n.º 13.709/18, resultando, pois, em uma análise que permite contrastar as previsões normativas anteriores com a nova previsão legal.

2. A EVOLUÇÃO DA PROTEÇÃO DE DADOS PESSOAIS

O direito à privacidade é personalíssimo e está estritamente ligado ao direito à intimidade e ao princípio da dignidade da pessoa humana. Por ser um direito fundamental, está previsto em importantes tratados e convenções internacionais, como a Declaração dos Direitos do Homem e do Cidadão (1789), a Declaração Universal dos Direitos do Homem (1948), a Convenção

Europeia dos Direitos do Homem (1950) e a Conferência Nórdica sobre o Direito à Intimidade (1967) (HIRATA, 2017), bem como no Código Civil brasileiro (2002) e, principalmente, na Constituição Federal do Brasil (1988), que prevê, no art. 5º, inc. X, que “são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito à indenização pelo dano material ou moral decorrente de sua violação.” (BRASIL, 1988).

As significativas mudanças sociais, decorrentes da incorporação das novas tecnologias, e o crescente uso da Internet como meio de comunicação basearam-se, sobretudo, na migração da economia da produção de bens para a economia do imaterial. Portanto, esse modelo se vale da coleta de dados pessoais e informações recolhidas e tratadas não somente para efetivar tais serviços, mas como poderosa fonte de insumos para as grandes empresas que atuam no segmento, fatores que tornam os direitos em discussão ainda mais vulneráveis. Essas mudanças fizeram com que as preocupações em torno do direito à privacidade deixassem de ser tratadas no âmbito eminentemente privado e individual, superando-se a ideia de que, para sua satisfação, bastaria a abstenção para avançar rumo ao reconhecimento de que as ameaças aos dados pessoais partem tanto de instituições públicas quanto privadas, de modo a ensejar um novo olhar para o tema.

É inegável que a sociedade ganhou um novo impulso com a chamada “era da informação”, que introduziu a reestruturação e organização de novos modos de ser e estar no mundo decorrentes dessa dinâmica realidade ditada pelas tecnologias, o que desencadeou a criação de mecanismos e ferramentas cada vez mais rápidas e eficazes na coleta e transmissão de dados (BIONI, 2019, p. 4). Essa facilidade em obter informações fez com que o direito à privacidade se tornasse um dos mais afetados, uma vez que a esfera privada cedeu espaço para que o avanço tecnológico ganhasse terreno (JORGETTO; CAVALCANTI, 2019, p. 36), o que não ocorreu sem fraturas. As novas formas de violação exigiram que se pensasse em outras estratégias de tutela e, considerando que os fluxos informacionais não respeitam as fronteiras do Estados, os contornos imprecisos da sociedade em rede exigem que se lance

um olhar atento aos mecanismos internacionais no que tange à proteção dos dados pessoais.

As primeiras legislações voltadas à proteção de dados são oriundas da União Europeia, e o marco desse surgimento foi na década de 70 do século XX, ocasião em que a Alemanha promulgou a Lei do *Land* alemão de Hesse, que tinha por objetivo "regular os bancos de dados informatizados de dados governamentais" (MACHADO, 2018, p. 123). No entanto, conforme Ruaro e Rodriguez (2010, p. 191), essa Lei não foi suficiente para fornecer as garantias previstas, pois a prática adotada por ela fez com que surgisse total insegurança na sociedade. Valendo-se dessa normativa, o Estado pretendia criar um censo que continha 160 (cento e sessenta) perguntas de cunho pessoal, voltadas à obtenção de dados referentes à vida profissional, ideologias políticas e crenças religiosas, informações que seriam confrontadas com dados contidos no registro civil. Quem não respondesse a esse censo estaria sujeito à multa, além de existir a possibilidade de os dados dessas pessoas serem encaminhados às autoridades federais.

Por conta da exposição e das sanções previstas, temia-se a criação de um "Estado superinformado" que, ao invés de ajudar o seu povo, estaria lhe prejudicando e isso acarretou a inconstitucionalidade do censo, conforme decidida pela Corte Constitucional, que entendeu que a diversidade de finalidades do censo impediria as pessoas de determinarem como seriam utilizados os seus dados. Ao analisar o tema sob essa perspectiva histórica, Ruaro e Rodriguez (2010, p. 191-192) explicam que:

> Este é o marco oficial em que surge da autodeterminação informativa, que seria, segundo a sentença, *o direito dos indivíduos decidirem por si próprios quando e dentro de quais limites seus dados pessoais poderão ser utilizados*. A partir desta idéia, o sujeito passa a poder decidir quando e sob que circunstâncias poder-se-á conhecimento de seus dados pessoais. Cabe ressaltar que o americano Alan Westin, já em 1967, falava nesta figura jurídica. No entanto, ainda que não desenvolvida *originariamente* pela própria Corte Constitucional, a Sentença da Lei do Censo é apontada pela maioria maciça da doutrina como uma referência na proteção de dados pessoais.

O marco histórico da proteção de dados pessoais criado na Alemanha também ficou evidenciado pelo surgimento da chamada autodeterminação informativa, que, da forma mais genérica, conceitua-se como o poder de decisão do indivíduo sobre a exibição e utilização de seus dados pessoais. Esse direito à autodeterminação informativa não se origina na legislação alemã, mas da construção jurisprudencial e dogmática baseada em valores intrínsecos a ela (ASSMANN, 2014, p. 20).

A abordagem doutrinária permite afirmar que o conceito de autodeterminação informativa não se limita apenas ao poder decisório do titular de direitos sobre suas informações pessoais, pois ele está estritamente ligado e dependente de outros elementos, como a autonomia e a liberdade, essenciais para o livre desenvolvimento da personalidade, como explica Assmann (2014, p. 21),

> A comunicação livre em uma sociedade democrática tem como requisito o livre desenvolvimento da personalidade para que haja um debate plural – cujas ideias postas em contraponto aperfeiçoam-se em um processo dialético. Instrumento necessário para concretização desses valores – constitucionalmente expressos – é o direito à autodeterminação informativa, que, enquanto direito fundamental, impõe limites ao Estado pela realização de suas dimensões negativa e positiva.

A autodeterminação informativa garante ao indivíduo o controle sobre seus dados, mas também possibilita que haja, entre os cidadãos e o Estado, o importante exercício da democracia, em que se estimula e valoriza a livre comunicação e a troca de ideias, até chegar a um senso comum que atenda às necessidades e limitações de ambas as partes.

Em adição à evolução histórica, pode-se dizer que em 1973 foi criado, na Suécia, o Estatuto para banco de dados, igualmente idealizado como uma espécie de censo para extrair e controlar o uso de dados pessoais pela população. Semelhante ao modelo sueco, em 1974 os Estados Unidos introduziram um banco de controle de dados, mas que, dessa vez, proibiria as agências governamentais de tornarem públicos esses dados ou repassá-los a outrem sem o prévio conhecimento de seus titulares (TAVARES; ALVAREZ, 2017, p. 166).

Essas previsões normativas eram consideradas como leis de primeira geração, e o seu foco principal era a concessão prévia de autorização, por parte do titular, para a criação de um banco de dados que, posteriormente, seria regulamentado pelos órgãos públicos que eram os principais, senão os únicos, interessados nessa forma de controle de dados. Porém, o que mais se temia era o uso indiscriminado dessas informações e as possíveis consequências que poderiam gerar, uma vez que "a estrutura e a gramática de tais leis era algo tecnocrático e condicionado pela informática – nelas, tratavam-se dos "bancos de dados", e não propriamente da "privacidade" (DONEDA, 2011, p. 96), o que significa dizer que o foco não era a proteção dos direitos fundamentais das pessoas envolvidas.

Devido à falta de estrutura das leis de primeira geração e por terem se tornado ultrapassadas, surgem, ainda na década de 70, as leis de segunda geração, dentre as quais podem-se citar a Constituição Portuguesa e a Constituição Espanhola, que tinham como preocupação principal a criação de sistemas que pudessem identificar quando os dados pessoais dos cidadãos estariam sendo mal utilizados. Logo, essa segunda onde produziu uma viragem normativa, pois, nas palavras de Pezzi (2007, p. 95),

> O foco deslocou-se do *hardware* que armazena os dados para a qualidade dos dados que estavam sendo armazenados. Isso ocorreu em razão da insatisfação dos cidadãos em verem seus dados, principalmente os sensíveis, sendo utilizados por terceiros de forma alheia a sua vontade. Exemplos dessa legislação podem ser encontrados na lei francesa de proteção de dados pessoais de 1978, denominada *informatique et Libertées*, a Lei Norueguesa de 1978, a Lei Suíça de 1981, a Lei da Islândia de 1981, a Lei de Luxemburgo de 1979 e o *Privacy Act* de 1974.

No mesmo sentido, Ruaro e Molinaro (2017, p. 21) explicam que "[...] a Constituição espanhola prevê, em seu artigo 18, a proteção dos cidadãos frente ao uso da informática. O dispositivo prevê que haverá uma limitação legal quanto ao uso da informática para garantir a honra, intimidade e o exercício pleno de direitos".

Desse modo, essas leis possibilitaram que o cidadão pudesse ter um controle mais preciso sobre a forma e a qualidade com que seus dados

estavam sendo utilizados, não se tratando apenas de autorizar ou não o seu fornecimento pelo Poder Público, mas também de identificar quando as suas informações pessoais estavam sendo mal utilizadas.

A rápida evolução informática determinou a intensificação da produção normativa e, já na década de 80, ocorre o avanço em direção às leis de terceira geração. Nessa nova fase, porém, fizeram-se necessárias algumas reflexões sobre os modelos adotados anteriormente, uma vez que nem todos lograram êxito devido a sua falta de flexibilidade diante do novo cenário tecnológico. Essas transformações foram essenciais para a compreensão de um novo conceito de privacidade e intimidade, que estavam a exigir um tratamento mais abrangente e que abarcasse os dados pessoais, visto que, havendo violação desses direitos, estaria também atingida e fragilizada a dignidade da pessoa humana (MACHADO, 2018, p. 125-126).

Nessa esteira, as leis de terceira geração se preocupariam não somente com a liberdade dos cidadãos em fornecerem seus dados pessoais, mas também valorizariam a autodeterminação informativa e os meios de efetivar essa liberdade, ainda que nem todos os cidadãos compreendessem a importância do tema e tivessem interesse em manter o controle sobre os dados, como explica Machado (2018, p. 126):

> Dessa forma, a participação do indivíduo nas leis de terceira geração fazia parte da sua estrutura. Todavia, nem todas as pessoas estariam dispostas a exercitar seu direito à autodeterminação informativa, seja por conta dos custos envolvidos, seja porque não tinham nem mesmo conhecimento sobre o uso dessas informações. Assim, a liberdade informacional continuava sendo um privilégio de uma minoria, que arcava com os custos desta proteção.

Passadas as três primeiras ondas de produção normativa, chega-se à geração das leis atuais, cuja promessa é suprir o que não foi possível com as legislações anteriores, que tinham como escopo o tratamento individual. Enquanto as primeiras gerações de leis buscavam, no próprio indivíduo, formas de proteger os dados pessoais, demonstrando como eles deveriam ou não fornecer esses dados; nessa nova etapa de produção normativa, o enfoque

passa a ser outro, isto é, de viés mais amplo e que envolve e responsabiliza a coletividade na proteção de dados pessoais (DONEDA, 2011, p. 98).

Ao fazer esse levantamento evolutivo, é impossível deixar de lançar as atenções para o Brasil, foco principal do presente estudo e país no qual falar sobre a proteção de dados pessoais envolve identificar uma série de legislações genéricas, insuficientes e de tardio desenvolvimento se comparado a outros países, tais como Argentina, que já possui regulamentação específica sobre o tema desde os anos 2000 (SILVA; SILVA, 2013, p. 16). Isso porque, em solo brasileiro, as primeiras demonstrações de proteção de dados pessoais surgiram com a previsão do *Habeas Data* no art. 5º, inc. LXXII da Constituição Federal. Além disso, ainda que tal previsão conferisse ao país certo pioneirismo na América Latina, ao estabelecer uma garantia constitucional específica sobre proteção de dados, posteriormente complementada pela previsão de proteção do banco de dados dos consumidores, previsto no art. 43 da Lei n.º 8.078/90 (PEZZI, 2007, p. 107), ficava muito aquém da proteção considerada suficiente e adequada.

Essa previsão do *Habeas Data* foi posteriormente regulamentada pela Lei n.° 9.507 de 1997, que, basicamente, prevê que o remédio constitucional será concedido para garantir à pessoa impetrante conhecimento e acesso às informações contidas em registros ou banco de dados de entidades governamentais ou de caráter público e, ainda, para retificação de dados quando o impetrante não quiser se valer da via judicial ou administrativa (art. 7º, incisos I e II) (BRASIL, 1997).

Mais tarde, foi criado o Projeto de Lei n.º 4.060 de 2012, que previa, em sua ementa, o tratamento de dados pessoais, mas que não teve sucesso em sua tramitação naquele momento, sendo arquivado no ano de 2015. Convém rememorar que “tal arquivamento deve-se à abertura de uma consulta pública pelo Ministério da Justiça em 28 de janeiro de 2015 com o objetivo de regulamentar o Marco Civil da Internet e de produzir um novo Anteprojeto de Lei de Proteção de Dados” (SILVA, 2015, p. 115).

Por conta disso e devido à ausência de legislação específica, a Lei n.º 12.965, de 2014, denominada Marco Civil da Internet, acabou suprindo

parcialmente essa lacuna ao prever, ainda que de maneira tímida, sobre a proteção de dados. Essa legislação "[e]stabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil" (BRASIL, 2014), o que também está previsto em seu art. 1.º. Além disso, prevê, em seu art. 3.º, inc. II, que um desses princípios é o da proteção da privacidade, conforme explica Silva (2015, p. 116),

> O Marco Civil buscou delimitar o tratamento jurídico da internet e, além de prever uma série de princípios gerais, estabeleceu diversos direitos e deveres dos envolvidos com a rede, e tratou de temáticas de naturezas diversas, partindo da questão da relação entre o Estado e os usuários da rede, regulamentando as obrigações dos provedores de acessos e referindo a proteção de dados pessoais.

Analisando essa Lei, é possível perceber que ela reforça a ideia de autodeterminação informativa (SILVA, 2015, p. 119), bem como o fato de a proteção de dados estar intimamente ligada ao princípio da dignidade da pessoa humana, pois carrega, em seus artigos, princípios fundamentais que reconhecem a importância dos direitos humanos e fundamentais, como, por exemplo, o disposto nos artigos 2.º e 7.º do Marco Civil da Internet (BRASIL, 2014).

Na concepção de Tavares e Alvarez (2017, p. 191),

> A finalidade do Marco Civil da Internet foi estabelecer princípios, garantias, deveres e direitos dos usuários de Internet, dos prestadores de serviços e do Poder Público, o que configurava antiga preocupação legislativa, como se extrai dos inúmeros projetos de lei que tramitavam nas duas casas do Congresso Nacional desde meados da década de 1990. E, exatamente pelo seu conteúdo principiológico, delimitador de diretrizes gerais para a regulação das questões decorrentes da relação entre o direito e a Internet, que, atualmente, é conhecido como a "Constituição da Internet".

Apesar de a Lei n.º 12.965/2014 ter amplo escopo e considerável previsão garantista baseada em princípios derivados da Constituição Federal, ela ainda deixou a desejar em alguns aspectos, notadamente quanto aos dados pessoais, como explica Machado (2018, p. 192),

> De fato, a Lei n.° 12.965/2014, denominada de Marco Civil da Internet, revela-se como avanço, fixando um marco histórico e jurídico de utilização da *web* no Brasil. Aplica-se a todas as situações em que esteja em perigo a privacidade do usuário, mas também tendo sido respeitada a liberdade de expressão das pessoas como direito igualmente integrante da personalidade humana. No entanto, verifica-se que, mesmo com o advento desta Lei, não se conseguiu resolver o problema da proteção dos dados pessoais.

Tal insuficiência não se traduz em descuido dos elaboradores, mas em opções possíveis no momento histórico de feitura da Lei, especialmente considerando a tensão existente entre os vários interesses em colisão. Diante disso, uma opção foi a aposta na redação mais aberta para os artigos, postergando-se, para um momento futuro, o tratamento de dados pessoais. Em outros pontos, houve uma mudança na tradição até então empreendida, o que, por certo, também impactou o tratamento dos dados pessoais, a exemplo do disposto nos artigos 18 e 19, que tratam da responsabilização civil dos provedores de aplicação por danos causados por terceiros, segundo os quais, só haverá a responsabilização se houver ordem judicial para determinar a supressão do conteúdo e essa for descumprida; do contrário, não haverá responsabilização do provedor de aplicação (BRASIL, 2014).

Após essa evolução histórica sobre as principais legislações internacionais e nacionais que tratam da proteção de dados pessoais, chega-se ao Projeto de Lei (PL) n.º 5.276, de 2016 (apensado ao Projeto de Lei n.º 4.060/2012), produção que teve a participação popular por meio de consulta pública, a que foi submetido antes de ser encaminhado para o Congresso Nacional. Esse PL dispôs sobre “tratamento de dados pessoais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural, pautado pelo princípio da não discriminação” (GONÇALVEZ; VARELLA, 2018, p. 523).

O Projeto de Lei n.º 5.276/2016 teve sua redação proposta a partir de uma Resolução criada pela Organização das Nações Unidas (ONU), datada do ano de 2013, que trata do "Direito à Privacidade na Era Digital”. O referido Projeto objetivou oportunizar que os titulares dos dados tivessem seu direito resguardado e, consequentemente, pudessem exercer o controle de suas próprias informações de forma a não se tornarem “reféns” da Internet. Além

disso, a elaboração desse projeto também teve forte influência das Diretivas da União Europeia, conforme explica Machado (2018, p. 194):

> Merece destaque a natureza principiológica dada ao Projeto de Lei n.° 5.276/16 (art. 6.º), com influência das Diretivas da União Europeia, sobretudo da Diretiva 95/46/CE. A proposta de lei trazia como base a previsão de dez princípios para a proteção de dados pessoais, tais como: finalidade, necessidade, livre acesso, proporcionalidade, qualidade de dados, transparência, segurança física e lógica, boa-fé objetiva, responsabilidade e princípio da prevenção.

Inicialmente, tanto o Projeto de Lei n.º 4060/12 quanto o Projeto de Lei n.º 5.276/16 tramitavam na Câmara de Deputados, porém o segundo "foi apenso ao PL 4060/12, que posteriormente transformou-se na Lei n.º 13.709/18" (MACHADO, 2018, p. 195). A edição da novel legislação traz consigo promessas e gera expectativas de que os dados pessoais sejam finalmente tutelados de maneira mais específica e adequada no Brasil, em atenção aos novos desafios que se apresentam pelo uso crescente das tecnologias da informação e comunicação. Dentre vários pontos que merecem atenção, a proteção aos dados pessoais sensíveis é uma das importantes previsões dessa Lei, ainda em período de *vacatio legis.* O tema ganha mais interesse e novos contornos quando o controlador é o Poder Público, conforme se verá no próximo tópico.

2.1 O TRATAMENTO DOS DADOS PESSOAIS EM PODER DA ADMINISTRAÇÃO PÚBLICA

Como foi possível constatar na primeira parte deste artigo, o Poder Público de outros países desempenhou e desempenha significativo papel no tratamento dos dados pessoais da população, como é caso abordado sobre o censo criado na Alemanha na década de 70. Os interesses que permearam o tema nem sempre coincidiram com a real proteção dos direitos dos titulares, a demonstrar a importância de se lançar um olhar crítico sobre a atuação do Estado.

No Brasil, a constante busca pela proteção de dados pessoais em poder da Administração Pública não é diferente, e um dos maiores desafios é o de atender às regras previstas na Lei n.º 12.527 de 2011, denominada de Lei de Acesso à Informação (LAI), conciliando a ideia de transparência pública com a proteção de dados pessoais, como explicam Ruaro e Molinaro (2017, p. 27),

> [...] cabe salientar que, em novembro de 2011, foi promulgada a Lei de Acesso à Informação – Lei n.° 12.527 -, estabelecendo o livre acesso a informações, a exceção das informações pessoais e as informações sigilosas. Seu objetivo é garantir o máximo de transparência aos atos da Administração Pública.

A informação é algo essencial para as sociedades democráticas e é direito de todos, principalmente quando se refere à atividade pública, cuja atuação deve ser norteada pelos princípios constitucionais da publicidade e moralidade. A transparência se reveste de dupla importância, e a divulgação de informações beneficia tanto a população quanto o Poder Público, na medida em que a sociedade, além de manter-se informada e em condições de exercer certo controle social, também servirá ao Poder Público para a proposição das políticas públicas a serem adotadas (MACHADO, 2018, p. 10).

Nesse mesmo sentido, Saldanha, Brum e Mello (2016, p. 473) argumentam:

> De fato, a informação é ferramenta indispensável de controle democrático das instituições, razão pela qual o direito à informação está ligado ao conceito de democracia participativa e respeito aos direitos fundamentais, de modo que a faculdade de comunicação e acesso à informação passam a ser formas irrenunciáveis de liberdade. Ocorre que, no mundo atual, as novas tecnologias da informação e comunicação figuram como instrumentos indispensáveis do acesso à informação em condições de igualdade pelos sujeitos sociais. Em outras palavras, a universalização do acesso às tecnologias informacionais é pré-condição da garantia dos direitos individuais de liberdade.

O acesso à informação se tornou indispensável, tanto para cumprir as exigências sociais de uma sociedade que quer ser informada sobre os atos que envolvem direitos e manutenção de deveres relativos à Administração Pública, quanto para o próprio Poder Público, que realiza a coleta dos mais diversos

dados sobre os quais tem interesse para a gestão pública. A informação está presente na relação democrática entre os indivíduos e entre estes e o Estado, o que é incrementado pelo uso crescente de tecnologias, que permitem a produção, distribuição e acesso a essas informações de forma cada vez mais célere. Resta saber se todo esse aparato tecnológico, bem como o recolhimento e o controle dos dados pessoais contribuem para fortalecer a democracia ou, ao revés, fragilizam os direitos fundamentais e a dignidade humana dos titulares, supedâneos dessa mesma democracia.

Convém lembrar que, para Bobbio e Bovero (2000, p. 386), existem diferentes definições de democracia, mas, em sua concepção, a melhor interpretação do termo diz respeito àquela em que o Poder Público é em público. O teórico utiliza-se dessa expressão “em público” para retratar “todos aqueles expedientes institucionais que obrigam os governantes a tomarem as suas decisões às claras e permitem que os governados vejam como e onde as tomam” (BOBBIO; BOVERO, 2000, p. 386).

Entende-se, a partir da visão de Bobbio e Bovero (2000, p. 386), que não há democracia se o poder for exercido de forma oculta, ou seja, para que o governo consiga estabelecer uma relação democrática com os cidadãos, deve tornar os seus atos e decisões públicos, de forma que nada seja feito sem passar pelo escrutínio dos maiores interessados, isto é, aqueles que os elegeram. A partir do exposto, é possível fazer uma aproximação desse pensamento com a LAI, pois seu objetivo é fazer com o que o Poder Público informe e seja transparente quanto a seus atos, prestando contas sobre suas decisões à população. Da mesma forma, deve atuar com relação ao tratamento de dados dos administrados.

A LAI regulamenta e normatiza o disposto na Constituição Federal de 1988, que estabelece, em seu art. 5º, inc. XIV, que “é assegurado a todos o acesso à informação e resguardado o sigilo da fonte, quando necessário ao exercício profissional” (BRASIL, 1988). Para tanto, a LAI adota os princípios da publicidade e transparência como essenciais para manter a sociedade informada sobre as atividades desenvolvidas pelo Poder Público. No entanto, quando se trata de dados pessoais, em poder da Administração Pública, esses

princípios têm de ser observados com mais cautela, visto que devem ser levados em consideração os princípios da intimidade, privacidade e confidencialidade das informações, como explica Doneda (2011, p. 103),

> A proteção de dados pessoais no ordenamento brasileiro não se estrutura a partir de um complexo normativo unitário. A Constituição Brasileira contempla o problema da informação inicialmente por meio das garantias à liberdade de expressão e do direito à informação, que deverão eventualmente ser confrontados com a proteção da personalidade e, em especial, com o direito à privacidade.

É preciso conciliar, então, transparência dos atos públicos com proteção de dados pessoais dos administrados e, apesar de parecer simples de entender os termos e garantias previstos na Lei, sustentar a publicidade como regra e o sigilo como exceção nem sempre é uma tarefa fácil de ser conciliada na prática. O problema se revela quando é necessário distinguir o que pode ser publicizado daquilo que é considerado sigiloso, o que consiste em um novo desafio para a Administração Pública, conforme explicitado por Gonçalves e Varella (2018, p. 518):

> Porém, ao prever a publicidade como regra e o sigilo como exceção, alguns órgãos e entidades da Administração Pública, no afã de se tornarem mais transparentes, cumprirem as novas regras e não sofrerem sanções de órgãos de controles governamentais, passaram a oferecer serviços que podem estar ferindo uma das exceções previstas no texto legal.

Assim, apesar de a LAI demonstrar avanço democrático ao fomentar o acesso à informação e a transparência da Administração Pública, as informações sensíveis, sem proteção específica à época, ficaram bastante fragilizadas (GONÇALVEZ; VARELLA, 2018, p. 516-517). Tal fato expõe, na opinião de Carvalho (2014, p. 117), a problemática tensão estabelecida entre o direito à informação e o direito à vida privada, entre o que pode se tornar público e o que deve ser preservado, conflito este que fica demonstrado na estrutura da Lei, cuja redação dos artigos 3º e 4º dá ênfase à prevalência do direito à informação sobre o da intimidade.

Constatado o problema, a forma mais usual de resolver esses conflitos de direitos fundamentais é, segundo Ardenghi (2012, p. 245), observando detidamente os contornos do caso concreto e sopesando a importância de cada um desses princípios, bem como a necessidade de sua aplicação, o que deve ser feito a partir de critérios como o da razoabilidade, que pode ser útil para avaliar qual deve prevalecer no caso concreto. Ainda que pareça uma boa alternativa, quando se trata de dados pessoais sensíveis, torna-se arriscado aplicar o critério da razoabilidade, uma vez que se está diante de informações de caráter sigiloso e pessoal, que envolvem direito de personalidade e que podem conduzir à discriminação do titular, por dizerem respeito à raça, nacionalidade, orientação sexual, opção religiosa, condição de enfermidade, dentre tantas outras informações que podem comprometer severamente o titular diante de sua publicização indiscriminada e, em alguns casos, irresponsável.

Analisando o conflito informação *versus* privacidade, no que diz respeito aos dados pessoais, principalmente ao se levar em conta os princípios que norteiam a Administração Pública, encontrou-se um problema fulcral: a falta de uma previsão legislativa específica que proteja esses dados e imponha ao Poder Público limites quanto à sua coleta e divulgação. Isso porque, no Brasil, a legislação vigente e ainda aplicável aos fluxos informacionais e à proteção de dados que estejam em repositórios digitais é a Lei n.º 12.965, de 2014, que, apesar de ter elevada posição no ordenamento jurídico quanto à proteção de direitos na Internet, não é específica em relação à proteção de dados e, portanto, teve de ser aplicada de forma subsidiária (BASTOS, 2018).

Convém lembrar que o Marco Civil da Internet foi desenvolvido com a finalidade de promover a proteção das relações que estavam surgindo através da Internet e teve, como principal motivo de sua criação, a inconformidade social com as tendências e intenções iniciais do Poder Legislativo implementar, por intermédio de leis penais, dando origem à regulamentação da Internet. Para evitar qualquer medida de caráter restritivo e inibitório, refletido pelas leis criminais, o Marco civil tratou de apresentar garantias e direitos baseados em

princípios que asseguram a liberdade no espaço virtual, mas também prevê, de maneira transversal, a preservação de dados pessoais (BIONI, 2019, p. 130).

Não obstante apresentar vários dispositivos que fazem referência a dados pessoais, com menção, inclusive, ao respeito à autodeterminação informativa, essa Lei está redigida de maneira muito ampla, não sendo possível aplicá-la a determinados casos específicos. Tais insuficiências são evidenciadas, principalmente, no que diz respeito ao tratamento dos dados pessoais em poder da Administração Pública, tema no qual ostenta lacunas a serem preenchidas, conforme explica Machado (2018, p. 108),

> Discute-se se o Marco Civil da Internet já não teria tratado satisfatoriamente da questão relativa à proteção de dados pessoais. A resposta é negativa, isto porque a citada lei tem como objetivo principal o uso da internet, fixando-se direitos e deveres dos usuários, no entanto, na parte que trata de proteção de dados pessoais, o faz de forma bem tímida, até porque não é este o seu foco principal, deixando ainda uma lacuna muito grande no que se refere a esta temática [...].

Mesmo tendo um caráter de proteção e prevendo formas de resguardar as informações pessoais, como é o caso da previsão do art. 7º, inc. VII da Lei, que disciplina que será assegurado aos usuários o direito a não terem seus dados fornecidos a outrem sem o seu consentimento, o Marco Civil da Internet não conseguiu resolver os problemas enfrentados na proteção de dados, pois não prevê formas de fiscalização ou sanções no caso de descumprimento dessa determinação (MENEGUIM, 2017).

Essa falta de regulamentação torna ineficaz e fragiliza a proteção de dados, visto que os programas de armazenamento e bancos de dados do Poder Público não são totalmente seguros, estando à mercê de invasões indevidas e vazamentos inesperados, dada à *expertise* e rapidez com que os *hackers* atuam. Um exemplo recente disso foi o vazamento de dados que estavam sob o poder do Conselho Nacional de Justiça (CNJ), ocorrido em abril de 2019, ocasião em que o referido órgão foi alvo de violações praticadas por *hackers* e usuários mal-intencionados, estimando-se que milhares de informações pessoais foram divulgadas indevidamente, tais como nome

completo, número de Cadastro de Pessoa Física (CPF), contas bancárias, entre outros (MUNIZ, 2019).

Esse e outros casos que ocorrem de forma frequente demonstram a importância do assunto, pois não há, na Lei n.º 12.965/14, amparo suficiente para proteger o titular dos dados, especialmente quando estes estão sob os cuidados do Poder Público. Tal constatação apontou para a necessidade de o Poder Legislativo editar uma lei específica sobre proteção de dados pessoais, que amplie o escopo de proteção das informações sensíveis, conforme será tratado a seguir.

2.1.1 INOVAÇÕES DA LEI N.º 13.709/18 E SEUS POSSÍVEIS REFLEXOS NA DISPONIBILIZAÇÃO DE DADOS PESSOAIS SENSÍVEIS EM PODER DA ADMINISTRAÇÃO PÚBLICA

Até o advento da Lei n.º 13.709, de 14 de agosto de 2018, não havia, no ordenamento jurídico brasileiro, legislação específica que regulamentasse adequadamente os dados pessoais sensíveis, mas apenas leis que tratavam dos dados pessoais de forma ampla, conforme evidenciado anteriormente.

Nos termos da novel legislação e seguindo os passos de legislações de outros países, em especial as emergentes da União Europeia, por dados pessoais sensíveis, entende-se todos aqueles que abrangem as informações de cunho íntimo de cada pessoa, tais como: convicções religiosas, filosóficas, origens raciais ou étnicas, orientação sexual, opiniões políticas ou dados relacionados à saúde (BRASIL, 2018).

Devido ao nível de intimidade presente nessas informações sensíveis, constata-se que seu tratamento inadequado, ou seja, sem o consentimento do titular e com a inobservância das cautelas necessárias, pode gerar inúmeros danos, uma vez que tais informações podem ser utilizadas para promover a intolerância, o preconceito ou a discriminação, violando direitos e garantias fundamentais dos titulares (MACHADO, 2018, p. 53).

Conforme já mencionado neste artigo, as violações aos dados pessoais estão suscetíveis a acontecer no âmbito público e privado, dado o avanço tecnológico e os mecanismos cada vez rápidos para se obter informações e coletar dados, o que pode ocorrer no processamento feito tanto por agentes públicos quanto por particulares. Um exemplo concreto dessa última atuação foi o vazamento de dados contidos na rede social *Facebook*, que foram utilizados irregularmente para impulsionar campanhas eleitorais nos Estados Unidos. Estima-se que, na ocasião, milhares de usuários foram atingidos e que esses dados foram acessados por uma empresa que trabalhava com campanhas eleitorais, que os utilizava para criar propagandas eleitorais e espalhar *Fake News*, a fim de manipular os eleitores estadunidenses, escândalo que serviu de alerta para toda a comunidade internacional (COÊLHO, 2019, p. 34-35).

A violação a essas informações sensíveis resulta em afronta a princípios como o da dignidade da pessoa humana, diretamente ferido quando ocorrem essas intromissões indevidas na privacidade dos titulares. Sobre esse princípio, Sarlet (2013, p. 20) explica:

> [...] a dignidade, como qualidade intrínseca da pessoa humana, é irrenunciável e inalienável, constituindo elemento que qualifica o ser humano como tal e dele não se pode ser destacado, de tal sorte que não se pode cogitar na possibilidade de determinada pessoa ser titular de uma pretensão a que lhe seja concedida a dignidade. Esta, portanto, compreendida como qualidade integrante e, em princípio, irrenunciável da própria condição humana, pode (e deve) ser reconhecida, respeitada, promovida e protegida, não podendo, contudo (no sentido ora empregado) ser criada, concedida ou retirada (embora possa ser violada), já que existe – ou é reconhecida como tal – em cada ser humano como algo que lhe é inerente.

Dessa forma, entende-se a dignidade como uma qualidade intrínseca à pessoa humana e como tal deve ser reconhecida por todos, além de respeitada e protegida, pois está suscetível a ser violada por práticas como estas, de invasão e exposição da intimidade e privacidade.

Para tentar frear essas violações, foi editada a Lei n.º 13.709 de 2018, conhecida como Lei Geral de Proteção de Dados (LGPD), que atualmente se encontra no período de *vacacio legis*, tendo sua vigência prevista para agosto

de 2020 (NUCCI; AQUINO, 2019), data que está sob discussão devido aos recentes fatos envolvendo a pandemia em curso. Essa Lei recebeu grande influência do Regulamento Europeu, denominado “General Data Protection Regulation” (GDPR), que entrou em vigor em 2018, apesar de ser uma evolução da Diretiva Europeia de 1995, e que foi um dos incentivos para que a Lei Geral de Proteção de Dados fosse promulgada, visto que, na ausência de legislação específica para regulamentar o tema – que já perdurava por muitos anos, o Brasil estaria impedido de receber dados transferidos de outros países (MACHADO; SANTOS; PARANHOS, 2018).

A partir de sua vigência, o tratamento dos dados pessoais será matéria exclusiva da Lei n.° 13.709, de 2018, que amplia sua proteção aos dados que se encontram nas plataformas digitais e aos que ainda se encontram em documentos físicos. Ademais, seu escopo é ampliado ao dispor sobre o tratamento feito por pessoas naturais, por pessoas de direito público ou privado, demonstrando que seu objetivo é preservar garantias de privacidade, liberdade e livre desenvolvimento da personalidade da pessoa natural, independentemente de quem é o responsável pela criação, coleta e tratamento dessas informações pessoais (BORELLI *et al.*, 2019, p. 19-20).

Ao analisar o texto da LGPD, logo no seu art. 2.º, é possível visualizar os fundamentos que inspiram e sustentam a proteção de dados e que são objeto do presente estudo, a saber: o respeito à privacidade (I); a autodeterminação informativa (II); a liberdade de expressão, de informação, de comunicação e de opinião (III); a inviolabilidade da intimidade, da honra e da imagem (IV); o desenvolvimento econômico e tecnológico e a inovação (V); a livre iniciativa, a livre concorrência e a defesa do consumidor (VI); e, por fim, os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais (VII) (BRASIL, 2018).

Todos esses fundamentos demonstram a preocupação do legislador em reforçar o direito à autodeterminação informativa, conferindo poder ao indivíduo para exercer sua escolha de consentir ou não com o uso de seus dados. Esse consentimento é fundamental para que os dados sejam utilizados e harmonizados com as necessidades e interesses que estão em pauta. Dessa

forma, só poderá ocorrer o seu tratamento depois que o seu titular for informado da necessidade dessa utilização e, a partir disso, seu consentimento deve ser dado de forma livre e expressa, por escrito ou por outro meio que seja possível comprová-lo (MACHADO, 2018, p. 200).

Apesar de existir essa previsão, que, em regra, deve ser sempre observada, a LGPD normatiza que, em casos excepcionais e necessários, será dispensada a exigência do consentimento expresso do titular. Assim, será dispensada a autorização quando os dados se tornarem manifestadamente públicos pela atuação do próprio titular e quando houver a necessidade de disponibilizá-los, levando-se em conta a finalidade, a boa-fé e o interesse público (art. 7.º, § 3.º e § 4.º) (BRASIL, 2018).

Nesse sentido, deve ser observado se há a real necessidade da utilização dos dados com a finalidade e o interesse públicos. Levando-se em conta que, nem sempre são considerados esses preceitos no tratamento dos dados pessoais, é necessária uma análise da sua aplicação para constatar se necessidade pública justifica a indispensabilidade do seu uso e publicização (BIONNI, 2019, p. 270). Portanto, é preciso analisar com cautela a necessidade dos dados pessoais, levando em conta a sua funcionalidade, uma vez que, conforme argumenta Coêlho (2019, p. 43),

> [...] é direito do possuidor dos dados a disponibilização clara, por meios facilitados, de como as suas informações pessoais estarão sendo utilizadas, nunca podendo os agentes de tratamento eximir-se desta responsabilidade. E não somente isso: o caráter de funcionalidade deve estar explícito na interação com o usuário, ou seja, a empresa deve dizer especificamente para que precisa das informações as quais solicita, onde as manuseia e para que fins haverá esta coleta. Toda a cadeia relacional deve estar pautada na boa-fé, zelo e cautela quanto ao usuário do serviço.

Para bem exercer o direito à autodeterminação, devem ser disponibilizadas todas as informações referentes à sua utilização aos titulares dos dados pessoais, para que estes saibam como serão extraídos, manuseados e aplicados os seus dados tendo em vista uma determinada finalidade. Porém, o que ainda deixa dúvidas, principalmente no que diz respeito ao tratamento conferido pelo Poder Público, é se a fiscalização desse

procedimento será realmente efetiva, o que vai desde o acesso à informação até o exercício da autodeterminação informativa dos titulares.

A Lei n.º 13.709, de 2018 apresenta uma conceituação necessária sobre o tema, principalmente no que diz respeito à diferenciação das expressões “dado pessoal” e “dado pessoal sensível”, para que não restem dúvidas quanto à interpretação de algum deles, visto que a primeira expressão abrange, de forma genérica, as informações pessoais de toda pessoa naturalmente identificada ou possivelmente identificável, enquanto que a segunda expressão se aplica às situações específicas. A partir da conceituação de dado sensível, conforme prevista no art. 5º, inc. II[1], pode-se interpretar, da melhor forma, o art. 11 e seus incisos, que tratam diretamente da proteção a esses dados e da limitação para seu uso (BRASIL, 2018).

O art. 11 prevê que nenhum indivíduo será obrigado a fornecer dados considerados sensíveis (conforme define a Lei), ou seja, em regra, esses dados só poderão ser fornecidos mediante autorização do titular, exceto quando o fornecimento for indispensável (II), como é o caso do “tratamento compartilhado de dados necessários à execução, pela Administração Pública, de políticas públicas previstas em leis ou regulamentos” (alínea b), ressalvando os direitos e garantias individuais (BRASIL, 2018).

A coleta de dados sensíveis ocorre tanto no âmbito público quanto no privado. Em relação ao primeiro, pode-se citar os formulários a serem preenchidos quando os participantes de programas governamentais na área da educação, por exemplo, precisam realizar sua inscrição mediante o preenchimento desses documentos, como é o caso do Exame Nacional do Ensino Médio (ENEM), que exige que o candidato preste informações consideradas sensíveis, como as de origem racial (GONÇALVEZ; VARELLA, 2018, p. 529). Já no âmbito privado, uma estratégia utilizada para obtenção de dados sensíveis diz respeito ao preenchimento de formulários prontos para a candidatura do funcionário ou durante a entrevista de emprego. Essas práticas são feitas com a finalidade de saber, previamente, se existe algum fator que

1 Art. 5º Para os fins desta Lei, considera-se:
II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

impeça a contratação de determinado candidato, mecanismo que invade a esfera privada individual (MACHADO, 2018, p. 198).

Em ambos os casos, a concessão dos dados confere grande responsabilidade por parte do ente público ou privado em armazená-los de forma segura, o que nem sempre acontece. Ciente disso, Machado (2018, p. 199) afirma que a nova Lei "[...] busca resgatar direitos valiosos à personalidade, como a privacidade informacional que, não obstante seja tutelada de forma genérica pela nossa Lei Maior, necessita de uma atenção especial por parte do legislador infraconstitucional [...]".

O tratamento específico dos dados pessoais pelo Poder Público está disciplinado do art. 23 ao art. 32 da LGPD e, conforme constata Bioni (2019, p. 245), a relação entre o Poder Público e os titulares das informações pessoais é marcada pela assimetria entre os atores, uma vez que o ente estatal sempre foi visto como detentor de posição de proeminência, devido ao fato de o interesse público possuir superioridade hierárquica em relação ao interesse individual. Portanto, pensar em mecanismos e alternativas, a fim de conferir poder ao titular dos dados, mostra-se adequado, pertinente e urgente, principalmente porque se sabe que os agentes públicos e governantes, historicamente, mantiveram bancos de dados com informações pessoais coletadas e utilizadas, muitas vezes, à revelia dos titulares.

O tratamento dos dados pessoais em poder da administração pública ficará a cargo das pessoas jurídicas de direito público, mencionadas no art. 1º, parágrafo único da LAI[2], e a LGPD impõe, como regra de utilização dessas informações, o dever de atender à finalidade pública, ou seja, a atuação deve ocorrer com base no interesse público e na execução de competências e atribuições legais do serviço público. Assim, quando o tratamento for feito pelo Poder Público, deverá ser observada, com rigor, a regra segundo a qual o

2 Art. 1º Esta Lei dispõe sobre os procedimentos a serem observados pela União, Estados, Distrito Federal e Municípios, com o fim de garantir 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.
Parágrafo único. Subordinam-se ao regime desta Lei:
I - os órgãos públicos integrantes da administração direta dos Poderes Executivo, Legislativo, incluindo as Cortes de Contas, e Judiciário e do Ministério Público;
II - as autarquias, as fundações públicas, as empresas públicas, as sociedades de economia mista e demais entidades controladas direta ou indiretamente pela União, Estados, Distrito Federal e Municípios.

fornecimento dos dados deverá ocorrer após seu titular possuir informações claras sobre o recolhimento e a utilização desses dados (BRASIL, 2018).

Outro ponto a se ressaltar nas mudanças introduzidas pela Lei de Proteção de Dados é o previsto no art. 26, § 1º, segundo o qual é vedado ao Poder Público transferir dados pessoais dos cidadãos de seus bancos públicos para entidades privadas, exceto nos casos em que há autorização expressa da Lei, como em contratos e convênios (IV). Havendo a transferência por essa razão, a autoridade nacional, embora ainda sem a devida constituição, deverá ser comunicada (§ 2º), o que permite evidenciar a importância que essa autoridade terá na fiscalização tanto dos atos do poder público quanto das instituições privadas (BRASIL, 2018).

A análise do texto legal permite constatar vetos feitos pela Presidência da República a algumas das sanções previstas no art. 52[3], em caso de descumprimento legal, o que leva Pinheiro (2018, p. 35) a supor que tal medida ocorreu no intuito de adequar a legislação à realidade do contexto social e econômico brasileiro, levando-se em conta a razoabilidade e a proporcionalidade, consequentemente, o que fez o Brasil não seguir à risca as disposições previstas no Regulamento Europeu. Diante disso, as sanções serão aplicadas somente depois de realizado o procedimento administrativo que oportuniza a abertura de prazo, para que o órgão que recolhe e trata as informações tenha a possibilidade de exercer a ampla defesa, e sua aplicação levará em conta a análise do caso concreto. A sanção considerará a análise de condicionantes, como a gravidade e a natureza da infração, o comportamento de boa-fé ou má-fé do agente, se houve a obtenção de alguma vantagem decorrente do ato, sua condição econômica e possível reincidência, entre outros fatores a serem considerados no caso concreto (BRASIL, 2018).

3 Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional:
I - advertência, com indicação de prazo para adoção de medidas corretivas;
II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;
III - multa diária, observado o limite total a que se refere o inciso II;
IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência;
V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
VI - eliminação dos dados pessoais a que se refere a infração.

Observa-se, durante a análise da Lei, que muitas vezes é mencionada a “Autoridade Nacional de Dados Pessoais” (ANDP), permitindo supor que esta desempenhará um papel de protagonista na aplicação dessas novas normas. A Autoridade Nacional é conceituada através do art. 5º, inc. XIX da LGPD, que a descreve como “órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei” (BRASIL, 2018).

A ANPD terá a função de regulamentar e fiscalizar os atos realizados no tocante aos dados pessoais, quer a atuação tenha ocorrido na esfera pública, quer na privada, aplicando as sanções pertinentes às infrações cometidas. Em razão de ter sido originariamente vetada na Lei, sua regulamentação ocorreu por Medida Provisória e está diretamente ligada à Presidência da República, o que compromete sua autonomia, ainda que a normativa de sua criação sustente em sentido contrário. Essa é uma das incoerências e lacunas da regulamentação, pois, conforme esclarece Coêlho (2019, p. 44),

> Outras lacunas preenchidas pela MP que merecem destaque dizem respeito à instituição e regulamentação do agir da Autoridade Nacional de Dados Pessoais (ANDP). Vetada pelo Presidente Michel Temer quando do sancionamento, para ser aprovada por medida provisória, fora alterada na sua essência de vinculação hierárquica, agora subordinada à própria Presidência da República, mas com a devida autonomia técnica. É função da ANPD não só reguladora, como sancionadora das penalidades que estão previstas no texto normativo. As multas a serem concedidas por atos infracionais à norma chegam a valores vultosos de cinco milhões de reais, por exemplo.

Essa novidade, apresentada pela Lei, demonstra a preocupação em ter um agente que fiscalize o tratamento dos dados pessoais, nas esferas pública e privada, e que, além de fiscalizar, também tenha autonomia para aplicar as sanções necessárias quando houver descumprimento das regras estabelecidas para o tratamento dessas informações.

A Autoridade Nacional é novidade para a legislação brasileira, haja vista que, em outros países, esse órgão já existia, inclusive, com poderes autônomos. A ideia dessa autoridade surgiu a partir da Diretiva Europeia de 1995, que previu sua criação nos países integrantes da União Europeia que não a possuíam. Seu surgimento foi de tamanha relevância que,

posteriormente, seu modelo foi aplicado em outros países não membros da União Europeia, como, por exemplo, Japão e Argentina (MACHADO, 2018, p. 208).

Embora demonstre um caráter inovador, a Autoridade Nacional ainda suscita dúvidas e receios, principalmente, sobre como será realizada a sua atuação prática. Isso implica uma certa insegurança por conta de, aparentemente, haver uma centralização de poder nas mãos desse órgão, o qual está subordinado à Presidência da República. Porém, por outro lado e reconhecendo a vulnerabilidade dos titulares dos dados pessoais, Machado, Santos e Paranhos (2018) sustentam que "é essencial que tenhamos uma Autoridade Nacional de Proteção de Dados incumbida de zelar pela sua aplicação, mas sobretudo nortear a sociedade em relação a como deve ser interpretada, seja no que se refere a aspectos jurídicos ou técnicos".

Apesar de os artigos 55, 56 e 57 da LGPD terem sofrido veto da Presidência da República, por conta de sua desconformidade com a regra que deveria passar pelo Poder Executivo e por previsão orçamentária antes de se tornar Lei, a Autoridade Nacional fora instituída através da Lei n.° 13.853, de 2019. Essa Lei dispõe sobre alterações feitas na Lei n.° 13.709, de 2018 e sobre a criação da Autoridade Nacional que, inicialmente, passa a ser um órgão integrante da Administração Pública Federal, subordinado à Presidência da República e passível de ter sua natureza jurídica reavaliada em até dois anos, por conta de seu caráter transitório (BRASIL, 2019).

Muitas são as atribuições da Autoridade Nacional, sendo uma delas enviar informes com previsão das medidas cabíveis para cessar possíveis violações advindas do tratamento dos dados em poder da Administração Pública, e, ainda, solicitar aos agentes detentores desses dados a publicação de relatórios que contenham informações sobre o impacto referente à proteção de dados e formas e sugestões de boas práticas relacionadas a essa proteção (BRASIL, 2018).

A Autoridade Nacional também poderá, sempre que necessário, solicitar aos órgãos e entidades do Poder Público a realização de operações de tratamento de dados pessoais, o fornecimento de informações específicas

referentes a esses dados, entre outros. Poderá, ainda, emitir parecer técnico complementar com o propósito de garantir o cumprimento do disposto na Lei (BRASIL, 2019).

Entre as competências da ANPD, estão as de zelar pela proteção dos dados pessoais e de elaborar diretrizes para a Política Nacional de Proteção de Dados e da Privacidade, de forma a inibir todo e qualquer ato de violação que possa partir dos agentes encarregados do tratamento das informações pessoais. Além dessas, há outras competências previstas no art. 55-J, que explicitam como será sua esfera de atuação, bem como a busca por certas garantias, a exemplo do tratamento de dados de idosos, para que seja efetuado da forma mais simplificada e clara possível, dispondo a eles acessibilidade, tudo em conformidade com o Estatuto do Idoso (BRASIL, 2019).

Além da Autoridade Nacional, outro agente criado pela nova Lei de Proteção de Dados é o encarregado, que atuará por indicação do controlador[4], constituindo-se numa espécie de mediador entre as partes interessadas no tratamento dos dados pessoais, ou seja, entre o controlador, o titular dos dados e a Autoridade Nacional, de forma a manter todos informados sobre os procedimentos realizados (art. 5º, inc. VIII) (BRASIL, 2018).

Por fim, a partir da análise da Lei n.º 13.709, de 2018, com enfoque voltado para o que é pertinente à Administração Pública, é possível visualizar várias propostas e inovações disciplinadas pela novel legislação, que valoriza a autodeterminação informativa, os direitos fundamentais e a proteção da esfera individual.

Além disso, com a criação da Autoridade Nacional, muitas são as expectativas relacionadas à fiscalização e ao cuidado no tratamento dos dados pessoais sensíveis, principalmente em face da atuação do Poder Público. Resta observar como este tratamento evoluirá, sobretudo diante da opção brasileira em vincular o órgão à Presidência da República, o que pode não só comprometer sua prometida autonomia como também colocar em risco a proteção de dados pessoais no Brasil.

4 Art. 5º Para os fins desta Lei, considera-se:
VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.

3. CONCLUSÃO

A nova Lei n.º 13.709, de 2018 é uma legislação com base principiológica, que evidencia que o Brasil começa a dar os passos iniciais em direção à proteção de dados, percorrendo a primeira etapa de uma longa trajetória já experimentada em outros países. Constitui-se em uma das mais esperadas leis a ser editada nos últimos tempos, tendo em vista a tardia evolução dessa proteção em território nacional.

Sua inspiração é claramente de origem europeia, baseando-se no Regulamento Europeu de Proteção de Dados, que é referência para vários países do mundo quando se trata desse tema, constituindo-se, igualmente, em um dos fatores impulsionadores da edição da novel legislação, sem a qual o Brasil teria problemas para negociar com as empresas europeias, justamente por não dispor de nível de proteção adequado aos parâmetros lá vigentes.

No decorrer desse estudo, observa-se que outros países estavam muito à frente do Brasil em relação a esse tema, a exemplo da Argentina, que mantém regulamentação específica desde os anos 2000, o que demonstra os anos de atraso do Brasil em comparação com seus países vizinhos. Esse atraso implicou também na violação a direitos fundamentais e ataques à dignidade da pessoa humana, uma vez que, para se exercer o efetivo direito à privacidade, principalmente a informacional, é necessário que o titular tenha autodeterminação informativa, conceito ainda em construção no país, cuja implementação e observância parecem distantes.

Com a edição e posterior implementação da Lei de Proteção de Dados, muitas foram as dúvidas que surgiram, principalmente no que diz respeito à aplicação de suas propostas inovadoras, sobretudo porque até então a proteção de dados era feita por legislações esparsas, dentre elas, a Lei n.º 12.965, de 2014, conhecida como Marco Civil da Internet. Tal legislação era aplicada de forma subsidiária e a fim de preencher as lacunas em razão da falta de uma lei específica. Porém, o Marco Civil da Internet não continha previsões específicas sobre dados pessoais sensíveis, a evidenciar a importância da legislação específica.

Além de regulamentar os dados pessoais sensíveis, novidade desta Lei, destaca-se a criação da Autoridade Nacional, existente em outros países. Sua criação foi idealizada com o intuito de ser um órgão autônomo e dotado de poderes de regulamentar, fiscalizar e aplicar sanções na esfera privada e pública, a fim de fazer valer o que está previsto na Lei. Como se sabe, sua criação foi inicialmente vetada, o que comprometeria a efetividade da recém criada Lei, situação contornada com a edição da Lei n.º 13.853, de 2019, que criou e regulamentou sua atuação, atribuindo-lhe diversas competências, dentre elas, o poder-dever de zelar pela proteção de dados. Ademais, normatiza como serão aplicadas essas competências e como será composta essa Autoridade, por meio de conselhos, ouvidorias e outros órgãos que possibilitem a aplicação das normas e regras dispostas na Lei.

Não obstante, todas essas previsões e as promessas de maior proteção, ainda assim há a preocupação em torno do tratamento dos dados em poder da Administração Pública, o que ocorre tanto em razão da assimetria de poder entre o Estado e seus órgãos e os cidadãos quanto em razão da necessidade de promover o acesso à informação, em atenção aos comandos da Lei de Acesso à Informação, que, em certa medida relativiza, essa proteção ao prever que a divulgação é a regra e o sigilo é a exceção.

Assim, embora apresente um regramento que se mostre adequado ao previsto na União Europeia, a nova Lei de Proteção de Dados ainda deixa a desejar quando o assunto é o tratamento dos dados pessoais sensíveis em poder da Administração Pública, uma vez que sua regulamentação apresenta mais disposições referentes ao setor privado do que em relação ao Poder Público. Em razão disso, estima-se que, com a vigência da Lei, a sua aplicação será interpretada conforme as necessidades do setor, o que nem sempre coincidirá com os direitos fundamentais dos cidadãos. Outro fator negativo é a centralização do poder em torno da Autoridade Nacional, principalmente pelo fato desta, inicialmente, ter ligação e subordinação direta à Presidência República, o que justifica a preocupação com relação ao risco de possível desvio de finalidade do referido órgão.

As dúvidas e insuficiências existentes até o momento não podem, no entanto, impedir o enaltecimento dos pontos positivos dessa legislação, que, se devidamente aplicada, poderá imprimir um novo comportamento nas organizações privadas e públicas, em respeito aos direitos fundamentais dos titulares de dados pessoais. Suas previsões, no entanto, constituem a primeira etapa de muitas que precisam ser trilhadas em direção ao empoderamento dos cidadãos e do desenvolvimento de uma cultura de respeito aos dados pessoais sensíveis por parte da Administração Pública, pois, como está redigida, é possível antever que a preocupação foi maior em proteger o cidadão na esfera privada, o que demonstra que ainda há muito para avançar rumo à proteção de dados pessoais por parte da Administração Pública brasileira.

REFERÊNCIAS

ARDENGHI, Régis Schneider. Direito à Vida Privada e Direito à Informação: Colisão de Direitos Fundamentais. **Revista da ESMESC**, Florianópolis, v. 19, n. 25, p. 227-251, 2012. Disponível em: https://revista.esmesc.org.br/re/article/view/57. Acesso em: 10 out. 2019.

ASSMANN, JHONATA. **O Direito à Autodeterminação Informativa no Direito Germânico e Brasileiro**. Orientador: Airton Lisle Cerqueira L. Seelaender. 2014. 65 f. Trabalho de Conclusão de Curso (Bacharelado em Direito) – Universidade Federal de Santa Catarina, Florianópolis, 2014. Disponível em: http://150.162.242.35/bitstream/handle/123456789/117169/Jhonata%20Assmann%20TCC%20pdfa.pdf?sequence=1&isAllowed=y. Acesso em: 10 set. 2019.

BASTOS, Athena. **Direito digital:** guia da Lei Geral de Proteção de Dados Pessoais (LGPD). 2018. Disponível em: https://blog.sajadv.com.br/direito-digital-lei-de-protecao-de-dados/. Acesso em: 17 out. 2019.

BIONI, Bruno Ricardo. **Proteção de Dados Pessoais**: a função e os limites do consentimento. Rio de Janeiro: Editora Forense, 2019.

BOBBIO, Norberto; BOVERO, Michelangelo (org.). **Teoria Geral da Política:** a filosofia política e as lições dos clássicos. Tradução Daniela Beccaccia Versiani. Rio de Janeiro: Campus, 2002.

BORELLI, Alessandra *et al*. LGPD: Lei Geral de Proteção de Dados comentada. *In:* MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (Coords.). São Paulo: Revista dos Tribunais, 2019.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, [2019]. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 12 maio 2019.

BRASIL, **Lei nº 9.507, de 12 de novembro de 1997**. Regula o direito de acesso a informações e disciplina o rito processual do *habeas data*. Brasília, DF: Presidência da República, [1997]. Disponível em: http://www.planalto.gov.br/ccivil_03/LEIS/L9507.htm. Acesso em: 20 set. 2019.

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. Brasília, DF: Presidência da República, [2011]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 22 maio 2019.

BRASIL. **Lei nº 12. 965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: Presidência da República, [2018]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 12 maio 2019.

BRASIL. **Lei nº 13.709/18, de 14 agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, [2018]. Disponível em: planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 20 maio 2019.

BRASIL. **Lei nº 13.853, de 8 de julho de 2019**. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. Brasília, DF: Presidência da República, [2019]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13853.htm. Acesso em: 28 out. 2019.

CARVALHO, Igor Chagas de. A tensão entre o direito à informação e o direito à privacidade e o acesso aos arquivos sensíveis. **Revista de Informação Legislativa**, Brasília, v. 51, n. 202, p. 115-130, abr/jun. 2014. Disponível em: https://www2.senado.leg.br/bdsf/handle/id/503040. Acesso em: 15 out. 2019.

COÊLHO, Amanda Carmen Bezerra. **A Lei Geral de Proteção de Dados Pessoais Brasileira Como Meio de Efetivação dos Direitos da Personalidade**. Orientador: Alfredo Rangel Ribeiro. 2019. 52 f. Trabalho de Conclusão de Curso (Bacharelado em Direito) - Universidade Federal da Paraíba, João Pessoa, 2019. Disponível em: https://repositorio.ufpb.br/jspui/bitstream/123456789/14305/1/ACBC05052019.pdf. Acesso em: 15 jun. 2019.

DONEDA, Danilo. A proteção de Dados Pessoais como um Direito Fundamental. **Revista Espaço Jurídico**, Joaçaba, v. 12, n. 2, p. 91-108, jul/dez. 2011. Disponível em: https://dialnet.unirioja.es/descarga/articulo/4555153.pdf. Acesso em: 22 maio 2019.

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: 16 maio 2019.

HIRATA, Alessandro. Direito à privacidade. *In:* VIDAL, Serrano Nunes Jr (Coords.). **Tomo: Direito Administrativo e Constitucional.** São Paulo: Pontifícia Universidade Católica de São Paulo, 2017. Disponível em: https://enciclopediajuridica.pucsp.br/verbete/71/edicao-1/direito-a-privacidade. Acesso em: 12 maio 2019.

JORGETTO, Leonardo Felipe de Melo Ribeiro Gomes; CAVALCANTI, Ana Elizabeth Lapa Wanderley. O Direito à Privacidade dos Dados Pessoais Sensíveis e os E-Mails Corporativos: Uma Visão sob o Aspecto dos Direitos da Personalidade na Sociedade da Informação. **Revista de Direito, Governança e Novas tecnologias**, Salvador, v. 4, n. 1, p. 33-50, jan/jun. 2018. ISSN: 2526-0049. Disponível em: https://www.researchgate.net/publication/327254882_o_direito_a_privacidade_dos_dados_pessoais_sensiveis_e_os_e-mails_corporativos_uma_visao_sob_o_aspecto_dos_direitos_da_personalidade_na_sociedade_da_informacao. Acesso em: 17 set. 2019.

MACHADO, Joana de Moraes Souza. **A tutela da privacidade na sociedade da informação**: a proteção dos dados pessoais no Brasil. Porto Alegre, RS: Editora Fi, 2018. *E-book*. Disponível em: https://www.editorafi.org/494joana. Acesso em: 12 maio 2019.

MACHADO, José Mauro Decoussau; SANTOS, Matheus Chucri dos; PARANHOS, Mario Cosac Oliveira. **LGPD e GDPR:** uma Análise Comparativa entre as Legislações. São Paulo, 2018. Disponível em: http://www.pinheironeto.com.br/publicacoes/lgpd-e-gdpr-uma-analise-comparativa-entre-as-legislacoes. Acesso em: 25 out. 2019.

MENEGUIM, Juliana. **Em pauta, a proteção a dados pessoais**. São Paulo, 2017. Disponível em: http://www.oabsp.org.br/noticias/2017/03/em-pauta-a-protecao-a-dados-pessoais.11571. Acesso em: 15 out. 2019.

MUNIZ, Mariana. CNJ sofre ataque hacker com vazamento de dados. **Valor econômico princípios editoriais**. Abr. 2019. Disponível em: https://www.valor.com.br/politica/6192567/cnj-sofre-ataque-hacker-com-vazamento-de-dados. Acesso em: 22 maio 2019.

NUCCI, Amanda Ferreira de Souza; AQUINO, Leonardo de. **Afinal, o que muda com a entrada em vigor da Lei Geral de Proteção de Dados Pessoais?**. 2019. Disponível em: http://www.justificando.com/2019/07/30/afinal-o-que-muda-com-a-entrada-em-vigor-da-lei-geral-de-protecao-de-dados-pessoais/. Acesso em: 28 out. 2019.

PEZZI, Ana Paula Jacobus. **A Necessidade de Proteção de Dados Pessoais nos Arquivos de Consumo:** em busca da concretização do direito à privacidade. Orientadora: Têmis Limberger. 2007. 216 f. Dissertação (Mestrado). Curso de Direito, Universidade do Vale do Rio dos Sinos – UNISINOS, 2007. Disponível em: http://www.dominiopublico.gov.br/download/teste/arqs/cp042824.pdf. Acesso em: 17 set. 2019.

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

RUARO, Regina Linden; MOLINARO, Carlos Alberto. Conflito real ou aparente de interesses entre o direito fundamental à proteção de dados pessoais e o livre mercado. *In:* RUARO, Regina Linden; MAÑAS, José Luis Piñar; MOLINARO, Carlos Alberto (Orgs.). **Privacidade e proteção de dados pessoais na sociedade digital**. Porto Alegre: Editora Fi, 2017. *E-book*. Disponível em: https://docs.wixstatic.com/ugd/48d206_22a63c4accd24433a0c23c09c909c77d.pdf. Acesso em: 13 maio 2019.

RUARO, Regina Linden; RODRIGUEZ, Daniel Piñeiro. O direito à proteção de dados pessoais na sociedade da informação. **Revista Direito, Estado e Sociedade Programa de Pós-Graduação em Direito da PUC-Rio**, Rio de Janeiro, n. 36, p. 191-192. 12 set. 2010. DOI: http://dx.doi.org/10.17808/des.36.212. Disponível em: https://revistades.jur.puc-rio.br/index.php/revistades/article/view/212/191. Acesso em: 13 maio 2019.

SARLET, Ingo Wolfgang. As dimensões da dignidade da pessoa humana: construindo uma compreensão jurídico-constitucional necessária e possível. *In:* SARLET, Ingo Wolfgang (Org.). **Dimensões da Dignidade**: Ensaios de Filosofia do Direito e Direito Constitucional. Porto Alegre, RS: Editora Livraria do Advogado, 2013.

SALDANHA, Jânia Maria Lopez; BRUM, Márcio Morais; MELLO, Rafaela da Cruz. As novas tecnologias da informação e comunicação entre a promessa de liberdade e o risco de controle total: estudo da jurisprudência do sistema interamericano de direitos humanos. **Anu. Mex. Der. Inter**, México, v. 16, p. 461-498, dic. 2016. Disponível em: http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1870-46542016000100461&lng=es&nrm=iso. Acesso em 10 out. 2019.

SILVA, Felipe Stribe da. **A proteção jurídica dos dados pessoais nos países do mercosul em face da segmentação comportamental:** um estudo

comparado. Orientadora: Rosane Leal da Silva. 2015. 167 f. Dissertação (Mestrado) - Curso de Direito, Universidade Federal de Santa Maria, Santa Maria- RS, 2015. Disponível em: https://repositorio.ufsm.br/handle/1/6381. Acesso em: 14 maio 2019.

SILVA, Letícia Brum da; SILVA, Rosane Leal. **A proteção jurídica dos dados pessoais na internet:** análise comparada do tratamento jurídico do tema na União Europeia e no Brasil, 2013. Disponível em: http://www.publicadireito.com.br/artigos/?cod=e4d8163c7a068b65. Acesso em 04 out. 2019.

TAVARES, Letícia Antunes; ALVAREZ, Bruna Acosta. Da proteção dos dados pessoais: uma análise comparada dos modelos de regulação da Europa, dos Estados Unidos da América e do Brasil. *In:* ONODERA, Marcus Vinicius Kiyoshi; FILIPPO, Thiago Baldani Gomes de (Coords.). **Brasil e EUA**: Temas de Direito Comparado. São Paulo: Escola Paulista da Magistratura, 2017. Disponível em: https://api.tjsp.jus.br/Handlers/Handler/FileFetch.ashx?codigo=94288. Acesso em: 17 set. 2019.

Recebido em | 27/05/2020
Aprovado em | 17/06/2020

Revisão Português/Inglês | Gabriela Quatrin Marzari

SOBRE AS AUTORAS | *ABOUT THE AUTHORS*

MARIANA ROCHA DE FLÔRES

Bacharela em Direito pela Antonio Meneghetti Faculdade (AMF). Pós-graduanda em Direito de Família e Sucessões pela Fundação Escola Superior do Ministério Público (FMP). Advogada. E-mail: adv.marianaflores@gmail.com.

ROSANE LEAL DA SILVA

Doutora em Direito pela Universidade Federal de Santa Catarina (UFSC). Professora Associada dos Cursos de Mestrado e de Graduação em Direito da Universidade Federal de Santa Maria. Atua como docente na Universidade Franciscana e na Antonio Meneghetti Faculdade, onde coordena o grupo de Pesquisa sobre Direito e Internet. Coordena o Núcleo de Direito Informacional (NUDI), da Universidade Federal de Santa Maria. E-mail: rolealdasilva@gmail.com.