FACULDADE ANTONIO MENEGHETTI
MARIANA ROCHA DE FLÔRES

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

RECANTO MAESTRO-RESTINGA SÊCA
2019

MARIANA ROCHA DE FLÔRES

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

Trabalho de Conclusão de Curso-Monografia, apresentado como requisito parcial para obtenção do título de Bacharel em Direito, Curso de Graduação em Direito, Faculdade Antonio Meneghetti-AMF.

Orientadora: Profª Drª Rosane Leal da Silva

RECANTO MAESTRO-RESTINGA SÊCA
2019

MARIANA ROCHA DE FLÔRES

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

Trabalho de Conclusão de Curso apresentado como requisito parcial para obtenção do grau de Bacharel em Direito, Curso de Graduação em Direito, Faculdade Antonio Meneghetti.

Orientadora: Profª. Drª Rosane Leal da Silva

COMISSÃO EXAMINADORA

Profª. Drª Rosane Leal da Silva
Orientadora
Faculdade Antonio Meneghetti-AMF

Prof. Ms. Mateus Renard Machado
Membro da Banca Examinadora
Faculdade Antonio Meneghetti-AMF

Bel. Andrey Oliveira Lamberty
Membro da Banca Examinadora
Faculdade Antonio Meneghetti-AMF

Recanto Maestro-Restinga Sêca, 08 de novembro de 2019.

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[1]

Mariana Rocha de Flôres[2]

Rosane Leal da Silva[3]

SUMÁRIO: Introdução; 1 A evolução da proteção de dados pessoais; 2 O tratamento dos dados pessoais em poder da administração pública; 3 Inovações da Lei 13.709/18 e os seus possíveis reflexos na disponibilização de dados pessoais sensíveis em poder da administração pública; Considerações Finais; Referências.

RESUMO: A Administração Pública compreende como princípios norteadores a transparência e a publicidade, conforme previsão contida no art. 5º, XIV da Constituição Federal e na Lei n. 12.527/2011, denominada de Lei de Acesso a Informação (LAI). Ocorre que, o seu âmbito de atuação está diretamente ligado a dados pessoais que não devem ser expostos ou publicizados, principalmente no que diz respeito aos dados pessoais sensíveis. Por conta disso, questiona-se se a disciplina dos dados pessoais sensíveis, recentemente regulada pela Lei n. 13.709/2018, se mostra adequada e suficiente quando o tratamento for feito pelo Poder Público. Na busca de enfrentar o tema e para nortear metodologicamente a investigação foram utilizados os métodos de abordagem dedutivo cumulado com os métodos de procedimento comparativo e histórico, desenvolvendo-se análise que envolve a evolução histórica da proteção dos dados pessoais, a manutenção destes em poder da Administração Pública, até se chegar a análise das possíveis mudanças encontradas na nova Lei. A partir do estudo realizado, conclui-se que a Lei n. 13.709/18 adentra o ordenamento jurídico com uma importante função social e garantista, apresentando diversos mecanismos inovadores em prol da proteção de dados pessoais. Todavia, no que diz respeito à proteção dos dados pessoais sensíveis em poder da Administração Pública, não se encontra na Lei Geral de Proteção de Dados amparo suficiente, tendo em vista que, sua normatização protetiva abrange muito mais a esfera privada, do que o poder público, demonstrando que ainda há muito que se avançar em relação a esse aspecto.

PALAVRAS-CHAVE: Administração Pública. Dados Pessoais Sensíveis. Lei nº 13.709/18. Proteção de Dados.

ABSTRACT: The Public Administration understands as guiding principles the transparency and the publicity, as foreseen in the art. 5, XIV of the Federal Constitution and Law no. 12.527/2011, called the Law on Access to Information (LAI). It turns out that its scope is directly linked to personal data that should not be exposed or publicized, especially with regard to sensitive personal data. Because of this, it is questioned whether the discipline of sensitive personal data, recently regulated by Law no. 13.709/2018, is adequate and sufficient when the treatment is done by the Government. In order to address the theme and to guide the research methodologically, the deductive approach methods used along with the

---

[1] Artigo apresentado como requisito parcial para aprovação na disciplina Trabalho de Conclusão de Curso II do Curso de Direito da Antonio Meneghetti Faculdade – AMF.

[2] Aluna da graduação em Direito da Antonio Meneghetti Faculdade – AMF. E-mail: maryfloores@hotmail.com

[3] Orientadora. Doutora em Direito pela Universidade Federal de Santa Catarina. Professora do Curso de Direito da Antonio Meneghetti Faculdade – AMF. E-mail: rolealdasilva@gmail.com.

comparative and historical procedure methods were developed, developing an analysis that involves the historical evolution of the protection of personal data, the maintenance of these in the power of Public Administration, until the analysis of the possible changes found in the new Law is reached. From the study, it can be concluded that Law no. 13.709/18 enters the legal system with an important social and guarantee function, presenting several innovative mechanisms for the protection of personal data. However, as far as the protection of sensitive personal data held by the Public Administration is concerned, the General Data Protection Law is not sufficiently supported, since its protective regulation covers the private sphere much more than the power demonstrating that much remains to be done in this regard.

KEY-WORDS: Public administration. Sensitive Personal Data. Law No. 13.709/18. Data protection.

INTRODUÇÃO

A proteção de dados pessoais no Brasil 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, aplicativos e sites de redes sociais que permitem a interação de forma rápida e incontrolável, nasce junto 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 o tempo todo.

Práticas habituais no cotidiano, como entrar em uma rede social, fazer um cadastro em um site de compras, em plataformas de currículos e até mesmo para participar de programas governamentais como, por exemplo, o Exame Nacional do Ensino Médio – ENEM - têm como exigência o fornecimento de informações pessoais. E, muitas vezes as pessoas não mensuram a extensão que produz a disponibilização das informações, bem como 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, mas o foco dessa 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, orientação sexual e informações confidenciais como referentes à

saúde. Sua disponibilização indevida pode servir como instrumento para o cometimento de discriminação, intolerância e constrangimento de seu titular.

A 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, 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. 13.709/2018 se mostra adequada e suficiente quando o tratamento for feito pelo Poder Público?

Com o intuito de responder a esta problemática, a pesquisa fora elaborada valendo-se do método de abordagem dedutivo, visto que parte-se da análise geral dos conceitos e marcos temporais que envolvem a proteção de dados pessoais, até se chegar aos seus desdobramentos específicos referentes aos dados sensíveis em poder da Administração Pública, o que é feito à luz da nova Lei n. 13.709/18.

Aliado ao método de abordagem dedutivo utilizou-se 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. 13.709/18, análise que permite contrastar as previsões normativas anteriores com a nova previsão legal.

Ademais, o trabalho seguirá a linha de pesquisa do Curso de Direito da Faculdade Antonio Meneghetti denominada Política, Direito, Ontologia e Sociedade, pois é feita a análise dos impactos da nova Lei de proteção de dados no âmbito da Administração Pública sempre que o tratamento dos dados pessoais sensíveis estiver sob sua responsabilidade.

1 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 na Constituição Federal do Brasil (1988) que prevê no art. 5º, X que “são invioláveis a

intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação.” (BRASIL, 1988).

Com as significativas mudanças sociais decorrentes novas tecnologias e do uso da internet como forma de comunicação, ampliação de serviços e fonte de aquisição de renda utilizando-se de informações e coleta de dados pessoais para efetivar esses serviços, tornou vulnerável esse direito. Essas mudanças fizeram com que as preocupações em torno do direito à privacidade deixassem de ser restritas somente a ameaças externas a esfera privada e passaram a ser maiores e voltados aos problemas de privacidade encontrados nos mais diversos meios de informação (MACHADO, 2018, p. 46).

A evolução social ganhou uma nova conjuntura com a era da informação, se reestruturando e se organizando de forma a se adequar a essa realidade tão avassaladora e implacável que são as tecnologias, utilizando-se desse novo momento para impulsionar o desenvolvimento econômico que antes era voltado apenas para os setores industriais e agrícolas. Com todo esse impulso, foram criados 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 o mais afetado, pois ficou ameaçado perante esse avanço desenfreado das redes. A esfera privada foi deixada de lado para que o avanço tecnológico ganhasse espaço (JORGETTO; CAVALCANTI, 2019, p. 36). Com o intuito de proteger esses direitos inerentes à pessoa tornou-se necessária a busca pela efetiva proteção através de uma evolução de mecanismos internacionais para a proteção dos dados pessoais.

As primeiras legislações voltadas à proteção de dados surgiram na União Europeia e o marco desse surgimento foi na década de 70 em que a Alemanha promulgou uma lei do *Land* 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 implementada na Alemanha não foi capaz o suficiente de fornecer as garantias previstas, pois a prática adotada por ela fez com que surgisse entre a sociedade total insegurança. Valendo-se da mesma, o Estado pretendia criar um censo que continha 160 perguntas de cunho pessoal voltadas a vida profissional, ideologias políticas e crenças religiosas, que seriam confrontadas com dados contidos no registro civil e quem não respondesse esse censo, estaria sujeito à multa, além de existir a possibilidade de os dados dessas pessoas serem encaminhados às autoridades federais.

Por conta disso, temia-se a criação de um “Estado superinformado” que ao invés de ajudar seu povo estaria os prejudicando e isso acarretou inconstitucionalidade do censo decidida pela Corte Constitucional que entendeu que a diversidade de finalidades do censo impediria as pessoas de determinarem como seriam utilizados seus dados. Com isso, 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 Westin47, 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 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).

Contudo, o conceito de autodeterminação informativa não se limita apenas a isso, ele está estritamente ligado e dependente de outros elementos como a autonomia e a liberdade, 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 preza a livre comunicação e a troca de ideias, até se chegar a um senso comum que atenda às necessidades e limitações de ambas as partes.

Em 1973 foi criado na Suécia o Estatuto para banco de dados, que também foi pensado como uma espécie de censo para extrair e controlar o uso de dados pessoais pela população. Semelhante a este 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 dos 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 para a criação de banco de dados que posteriormente seriam regulamentados pelos órgãos públicos que eram os principais, se não, 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).

Devido à falta de estrutura das leis de primeira geração e por terem se tornado ultrapassadas, surge ainda na década de 70 as leis de segunda geração, dentre as quais pode-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 e, nas palavras de Pezzi (2007, p. 95):

> O foco deslocou-se do *hadware* 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, explicam Ruaro e Molinaro (2017, p. 21) que "[...] a Constituição espanhola prevê, em seu artigo 18, a proteção dos cidadãos frente o 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".

Dessa forma, essas leis possibilitaram que o cidadão pudesse ter um controle mais preciso sobre a qualidade em que estavam sendo utilizados seus dados, não se tratando apenas de autorizar ou não o seu fornecimento pelo poder público, mas era possível identificar quando as suas informações pessoais estavam sendo mal utilizadas.

Já na década de 80 se chega às leis de terceira geração, nessa nova fase fizeram-se necessárias algumas reflexões sobre os modelos adotados anteriormente que nem todos lograram êxito devido a sua falta de flexibilidade e também por conta dos avanços encontrados nas tecnologias de informática em rede. Esses avanços tecnológicos foram

essenciais para entender que a privacidade e a intimidade deveriam ter um tratamento mais abrangente, sendo necessária maior proteção aos dados pessoais, visto que, havendo violação a esses direitos, estaria também violando a dignidade da pessoa humana (MACHADO, 2018, p. 125-126).

Assim sendo essas leis de terceira geração se preocupariam não somente com a liberdade dos cidadãos em fornecerem seus dados pessoais, aqui se entra novamente no ponto da autodeterminação informativa, mas, em efetivar essa liberdade, apesar de nem todos os cidadãos terem interesse sobre isso, 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 gerações chega-se à geração das leis atuais, conhecida como quarta geração, que tem por objetivo suprir o que não foi possível com as legislações anteriores, que tinham como escopo o tratamento individual. Assim sendo, buscavam no próprio indivíduo formas de proteger os dados pessoais demonstrando como eles deveriam ou não fornecer esses dados. Assim com a nova geração, o enfoque passa a ser outro, um novo modelo que envolve a coletividade na busca da proteção aos dados pessoais (DONEDA, 2011, p. 98).

No Brasil, foco principal do presente estudo, falar sobre o tema da proteção de dados pessoais envolve uma série de legislações genéricas, insuficientes e de tardio desenvolvimento, comparado a outros países como Argentina que já tem regulamentação específica sobre o tema desde os anos 2000 (SILVA; SILVA, 2013, p. 16). Isto porque, as primeiras demonstrações de proteção de dados pessoais surgiram com a previsão do *habeas data* no art. 5º, inc. LXXII da Constituição Federal – apesar de isso ter feito com que ele se tornasse pioneiro na América Latina a estabelecer uma garantia constitucional específica sobre proteção de dados, e com o banco de dados dos consumidores previsto no art. 43 da Lei 8.078/90 (Código de Defesa do Consumidor) (PEZZI, 2007, p. 107).

No mesmo viés explica Doneda (2011, p. 103),

> [...] a Constituição [...] instituiu a ação de habeas data (art. 5º, LXXII), que basicamente estabelece uma modalidade de direito de acesso e retificação dos dados pessoais. Na legislação infraconstitucional, destaque-se o Código de Defesa do Consumidor, Lei 8.078/90, cujo artigo 43 estabelece uma série de direitos e

> garantias para o consumidor em relação às suas informações pessoais presentes em "bancos de dados e cadastros", implementando uma sistemática baseada nos Fair Information Principles à matéria de concessão de crédito e possibilitando que parte da doutrina verifique neste texto legal o marco normativo dos princípios de proteção de dados pessoais no direito brasileiro.

Essa previsão do *Habeas Data* foi posteriormente regulamentada pela Lei 9.507 de 1997, que basicamente prevê que o este será concedido para garantir a pessoa impetrante, conhecimento e acesso a 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, I e II) (BRASIL, 1997).

Mais tarde, foi criado o Projeto de Lei nº 4.060 de 2012, que previa em sua ementa o tratamento de dados pessoais, porém que não teve sucesso naquele momento, pois foi arquivado no ano de 2015, "tal arquivamento deve-se a 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, a lei que ficou conhecida por ser o Marco Civil da proteção de dados no Brasil foi a Lei nº 12.965 de 2014 que demonstra através de sua ementa que "Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil" (BRASIL, 2014) o que também está previsto em seu art. 1º. Além disso, prevê em seu art. 3º, 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) e 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 demonstram isso como por exemplo, o "Art. 2º A disciplina do uso da internet no Brasil tem como fundamento o respeito à liberdade de expressão, bem como: II - os direitos humanos, o desenvolvimento da personalidade e o exercício da cidadania em meios digitais" e o "Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos" (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 12.965/2014 ter sido denominada o Marco Civil da internet devido a sua considerável previsão garantista baseada em princípios norteados pelas leis anteriores e pela Constituição Federal, ela ainda deixou a desejar em alguns aspectos 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.

Isso acontece porque ela demonstra em seus artigos uma proteção muito ampla, não havendo previsões específicas sobre determinadas situações em que há violação a dados pessoais o que a torna frágil em alguns aspectos. Um exemplo disso se encontra no art. 18 e 19 que trata da responsabilização civil por danos causados por terceiros em que prevê que só haverá a responsabilização se houver ordem judicial a respeito e essa for descumprida, do contrário não haverá responsabilização do provedor de conexão à internet (BRASIL, 2014).

Após todo esse apanhado geral das principais legislações internacionais e nacionais a tratar de proteção a dados pessoais dentro e fora do Brasil, chega-se ao Projeto de Lei nº 5.276 de 2016 (apensado ao Projeto de Lei nº 4.060/2012) que é um projeto em que teve a participação do povo através de uma 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" (GONCALVEZ; VARELLA, 2018, p. 523).

O Projeto de Lei nº 5.276/2016 foi pensado a partir de uma Resolução criada pela Organização das Nações Unidas (ONU) em 2013 que trata do "Direito à Privacidade na Era Digital", com o intuito de dar a oportunidade aos seus titulares de terem direito e controle de suas próprias informações de forma a não se tornarem "reféns" da internet. Além disso,

também teve fortes influências 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. 6º), 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 nº 4060/12 quanto o Projeto de Lei nº 5.276/16 tramitavam na Câmara de deputados, porém o segundo "foi apenso ao PL 4060/12, que posteriormente transformou-se na Lei 13.709/18" (MACHADO, 2018, p. 195). E com o surgimento dessa nova Lei vem junto as expectativas de que o que antes era pouco regulamentado ou regulamentado de forma muito ampla, não cabendo para casos específicos, se torne mais delimitado, mais adequado ao tratamento jurídico necessário que requer esse tema, que é tão importante a sociedade. A proteção aos dados pessoais sensíveis é novidade dessa Lei, que está passando pelo período de *vacatio legis*, mas isso será abordado de forma mais específica nos próximos pontos desse estudo.

2 O TRATAMENTO DOS DADOS PESSOAIS EM PODER DA ADMINISTRAÇÃO PÚBLICA

Como se pode ver no capítulo anterior, o Poder Público de outros países tem uma significativa história referente ao tratamento dos dados pessoais de sua população, como é caso abordado sobre o censo criado na Alemanha na década de 70, mas que nem sempre surtiram os resultados esperados. No Brasil, a constante busca pela proteção de dados pessoais em poder da administração pública não é diferente, e um dos maiores desafios encontrados é o de atender as regras encontradas na Lei de Acesso a Informação nº 12.527 – LAI promulgada em 18 de novembro de 2011, 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 a sociedade e é direito de todos, principalmente no que diz respeito a atividade pública e isso ocorre de ambos os lados. As informações beneficiam tanto a população quanto o poder público, pois é seu dever manter as pessoas

informadas do trabalho desenvolvido, bem como das propostas e medidas futuras, mas também é através das informações e dados coletados que se torna possível que sejam pensadas as políticas públicas a serem adotadas (MACHADO, 2018, p. 10).

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

> 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.37 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 se utiliza desse direito quando se trata da coleta dos mais diversos dados pelos quais tem interesse. A informação está presente na relação democrática entre indivíduo e Estado e as tecnologias estão possibilitando a produção, distribuição e acesso a essas informações de forma cada vez mais célere.

Para Bobbio (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, utilizando-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, 2000, p. 386).

Entende-se a partir da visão de Bobbio (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 seu povo, deve tornar os seus atos e decisões públicos, de forma que nada seja feito sem passar pelos olhos dos maiores interessados, aqueles que os elegeram. Com base nisso, é possível fazer um paralelo desse pensamento com a Lei de Acesso a informação, pois seu objetivo é fazer com o que o Poder Público informe e seja transparente quanto a seus atos, prestando contas sobre suas decisões.

A Lei de Acesso a Informação (LAI) disciplina o direito ao acesso à informação assegurado inicialmente na Constituição Federal de 1988, que estabelece em seu art. 5º, XIV que “é assegurado a todos o acesso à informação e resguardado o sigilo da fonte, quando necessário ao exercício profissional” (BRASIL, 1988).

Isto posto, a LAI prevê em seu texto os princípios da publicidade e transparência que são 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 tem que ser observados com mais cautela, visto que tem que ser levados em consideração os princípios da intimidade, privacidade e da 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 expressão35 e do direito à informação,36 que deverão eventualmente ser confrontados com a proteção da personalidade e, em especial, com o direito à privacidade.

No art. 3º, caput da LAI é possível visualizar a previsibilidade de aplicação desses princípios quando dispõe que "os procedimentos previstos nesta Lei destinam-se a assegurar o direito fundamental de acesso à informação e devem ser executados em conformidade com os princípios básicos da administração pública e com as seguintes diretrizes" dentre os mesmos já prevê no inciso I a "observância da publicidade como preceito geral e do sigilo como exceção" (BRASIL, 2011).

Apesar de parecer simples de entender os termos e garantias previstos na Lei, quando se fala em publicidade como regra e sigilo como exceção, não é. O problema é encontrado quando se tem que separar o que pode ser publicizado e o que é considerado sigiloso e isso se torna um desafio para administração pública. Além disso, uma das regras encontradas na Lei ainda no art. 3º, IV é o fomento ao desenvolvimento da cultura de transparência na administração pública, o que faz com que os órgãos públicos busquem ao máximo cumprir com o estabelecido, como frisa 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.

Apesar de a LAI demonstrar um grande avanço democrático com o fomento ao acesso à informação e transparência da administração pública, por outro lado isso torna mais vulnerável o tratamento dos dados pessoais que estão em poder da administração pública, principalmente no que diz respeito as informações sensíveis que não eram regulamentadas por lei específica antes (GONÇALVEZ; VARELLA, 2018, p. 516-517).

Segundo Carvalho, (2014, p. 117), a Lei de Acesso a informação demonstra em seu texto legal 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 e isso fica demonstrado na estrutura da Lei, reforçando o previsto no art. 3º e art. 4º da mesma, que dão ênfase a prevalência do direito à informação sobre o da intimidade.

Sendo assim, conforme Ardenghi (2012, p. 245) a forma mais usual de resolver esses conflitos de direitos fundamentais é observando, no caso concreto, a importância de cada um desses princípios e a necessidade de aplicação, utilizando-se de critérios para avaliar qual deve prevalecer, como por exemplo, o critério da razoabilidade.

Porém, quando se trata de dados pessoais sensíveis se torna arriscado aplicar o critério da razoabilidade, uma vez, que se trata de informações de caráter sigilo e pessoal, que envolvem direito de personalidade, não podendo ser comprometidos por uma publicização indiscriminada e, em alguns casos, irresponsável.

Analisando esse conflito informação vs. privacidade no que diz respeito aos dados pessoais, principalmente por conta dos princípios que norteiam administração pública, encontrou-se um problema crucial, a falta de previsão legislativa específica que proteja esses dados e imponha ao poder público limites quanto a coleta e divulgação dos mesmos. Isso porque no Brasil (anterior a vigência da nova Lei de proteção de dados) a legislação aplicável a proteção de dados é a Lei n. 12.965 de 2014, considerada marco civil da internet, apesar de ter uma posição importantíssima no ordenamento jurídico quando se trata de evolução na proteção de dados pessoais, não é específica sobre o tema e teve de ser aplicada de forma subsidiária na falta de Lei específica (BASTOS, 2018).

A Lei considerada marco civil da internet foi desenvolvida 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 o fato de existir a ideia de o Poder Legislativo implementar, por intermédio de Leis Penais, a regulamentação da internet. Para evitar qualquer tipo de caráter restritivo e inibitório refletido pelas Leis criminais, essa Lei apresenta garantias e direitos baseados em princípios que asseguram a liberdade no espaço virtual, mas também prevê a preservação de dados pessoais (BIONI, 2019, p. 130).

Essa Lei n. 12965/14 apesar de apresentar vários dispositivos que tratam dos dados pessoais, inclusive, no que diz respeito a autodeterminação informativa, é detentora de uma regulamentação muito ampla, não sendo possível aplicá-la a determinados casos específicos, principalmente no que diz respeito aos dados pessoais em poder da Administração Pública, mantendo 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, VII da lei, que disciplina que será assegurado aos usuários o direito de não ter seus dados fornecidos a outrem se não pelo seu consentimento, o marco civil da internet não conseguiu resolver os problemas enfrentados na proteção de dados, visto que, não prevê formas de fiscalização ou sanções no caso de descumprimento dessa determinação (MENEGUIM, 2017).

Essa falta de regulamentação torna, de certa forma, ineficaz a proteção de dados, pois os programas de armazenamento e bancos de dados do poder público não são totalmente seguros, estando a mercê de vazamentos inesperados, dada a expertise e rapidez com que os hackers atuam, um exemplo recente disso foi o vazamento de dados que estavam sob poder do Conselho Nacional de Justiça (CNJ). Em abril de 2019, o CNJ foi alvo de violações praticadas por hackers e usuários mal-intencionados e estima-se que milhares de informações pessoais foram vazadas como: nome completo, CPF, contas bancárias, entre outros (MUNIZ, 2019).

Esse e outros casos que ocorrem de forma frequente demonstram tamanha importância do assunto, pois havendo esse tipo de violação, não há na Lei n. 12.965/14, amparo suficiente para aplicar as sanções necessárias. Sendo o poder público detentor de informações pessoais totalmente sigilosas e que se usadas de forma errada podem comprometer a vida das pessoas, houve a necessidade de o Poder Legislativo implementar uma Lei específica sobre proteção de dados pessoais, que regulamente os dados pessoais sensíveis como veremos a seguir.

3 INOVAÇÕES DA LEI 13.709/18 E OS SEUS POSSÍVEIS REFLEXOS NA DISPONIBILIZAÇÃO DE DADOS PESSOAIS SENSÍVEIS EM PODER DA ADMINISTRAÇÃO PÚBLICA

Até o advento da Lei 13.709/18 não havia no ordenamento jurídico legislação específica que abordasse o conceito ou regulamentasse os dados pessoais sensíveis, somente

haviam leis que tratassem do tema dados pessoais de forma ampla como já visto anteriormente.

Por dados pessoais sensíveis entende-se todos os que abrangem informações de cunho íntimo de cada pessoa como: convicções religiosas, filosóficas, origens raciais ou étnicas, orientação sexual, opiniões políticas ou dados relacionados a saúde (BRASIL, 2018).

Devido ao nível de intimidade que tem essas informações sensíveis, quando fornecidas de forma inadequada e sem consentimento podem gerar inúmeros danos, uma vez que podem ser utilizadas para promover a intolerância, preconceito ou discriminação violando direitos e garantias fundamentais (MACHADO, 2018, p. 53).

Conforme já mencionado nesse estudo, as violações aos dados pessoais estão suscetíveis a acontecer no âmbito público e privado, dado ao avanço tecnológico e aos mecanismos cada vez rápidos para obter informações e coletar dados, mesmo que de forma ilegal. Um exemplo concreto disso foi o vazamento de dados contidos na rede social *Facebook*, que foram utilizados irregularmente para impulsionar campanhas eleitorais nos Estados Unidos. Estima-se que milhares de usuários foram atingidos e que esses dados estariam sendo utilizados por uma companhia que trabalhava com campanhas eleitorais, que os utilizava para criar propagandas eleitorais e espalhar *Fake News* a fim de manipular os eleitores estadunidense, escândalo que serviu de alerta para toda comunidade internacional (COÊLHO, 2019, p. 34-35).

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

> [...] 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 intrínseca à pessoa humana e como tal deve ser reconhecida por todos, respeitada e protegida, pois está suscetível a ser violada por práticas como estas de invasão e exposição da intimidade e privacidade.

A Lei 13.709/18 conhecida como Lei Geral de Proteção de Dados, foi promulgada em 14 de agosto de 2018 e atualmente ainda se encontra no período de *vacacio legis*, tendo sua vigência prevista para agosto de 2020 (NUCCI; AQUINO, 2019). Essa Lei tem grandes influências do Regulamento Europeu "General Data Protection Regulation" (GDPR) que entrou em vigor em 2018 (apesar de ser uma evolução da Diretiva Europeia de 1995) e 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).

O tratamento dos dados pessoais é matéria exclusiva da Lei 13.709/18, que amplia sua proteção aos dados que se encontram nas plataformas digitais e aos que não estão, ou seja, os que ainda se encontram em documentos físicos. Além disso, sua regulamentação dispõe sobre o tratamento feito por pessoas naturais, mas também 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, tendo em vista a vulnerabilidade dos titulares dos dados em relação aos agentes que criam, coletam e fazem o tratamento dessas informações pessoais (BORELLI et al, 2019, p. 19-20).

Ao analisar a LGPD, logo no seu art. 2º é possível visualizar os fundamentos que permeiam a proteção de dados e que são objeto desse estudo, sendo eles: 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; os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais (VII) (BRASIL, 2018).

Todos esses fundamentos reforçam a preocupação do legislador em reforçar nessa Lei o direito que o indivíduo tem de exercer sua escolha de consentir ou não com o uso de seus dados. Esse consentimento é fundamental para que esses dados sejam utilizados e harmonizados com as necessidades e interesses que estão em pauta. Dessa forma, só poderá ocorrer o tratamento dos dados pessoais depois que o seu titular for informado da necessidade dessa utilização, a partir disso, o consentimento deste deve ser dado de forma livre e expressa, por escrito ou por outro meio que seja possível comprovar esse consentimento para que não restem dúvidas (MACHADO, 2018, p. 200).

Apesar de existir essa previsão que, em regra, deve ser sempre observada e levada em consideração, a LGPD normatiza que em casos excepcionais e necessários, será dispensada a exigência do consentimento ora previsto. Não será necessário o consentimento do titular dos dados quando estes se tornarem manifestadamente públicos por eles mesmos e quando houver a necessidade de disponibilizá-los levando-se em conta a finalidade, a boa-fé e o interesse público (art.7º, § 3º e § 4º) (BRASIL, 2018).

Nesse sentido, deve ser observado se há a real necessidade da utilização dos dados com a finalidade e interesse público, levando-se em conta que nem sempre são considerados esses preceitos no tratamento dos dados pessoais, sendo necessária uma análise da sua aplicação, se a necessidade pública justifica a indispensabilidade do seu uso e publicização (BIONNI, 2019, p. 270).

Nas palavras de 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.

Aos titulares dos dados pessoais devem ser disponibilizadas todas as informações referentes a utilização desses, de forma que saibam como serão extraídos, manuseados e aplicados para determinada finalidade. Porém, o que ainda deixa dúvidas, principalmente no que diz respeito ao tratamento dado pelo Poder Público, é se realmente será efetiva a fiscalização desse procedimento, o que vai desde o acesso à informação até o exercício da autodeterminação informativa dos titulares.

A Lei 13.709/18 apresenta uma conceituação necessária sobre o tema, principalmente no que diz respeito a diferenciação das expressões “dado pessoal” e “dado pessoal sensível” para que não restem dúvidas na interpretação de algum deles, visto que, a primeira expressão abrange de forma expansiva as informações pessoais de toda pessoa natural identificada ou possivelmente identificável, enquanto a segunda expressão se aplica a situações específicas. A partir da conceituação de dado sensível prevista no art. 5º, II[4], pode-

[4] 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;

se interpretar da melhor forma o art. 11 e seus incisos que tratam diretamente da proteção a esses dados e a limitação para uso dos mesmos (BRASIL, 2018).

O art. 11 prevê que nenhum indivíduo será obrigado a fornecer dados considerados sensíveis (conforme a lei), ou seja, em regra só poderão ser fornecidos mediante autorização do mesmo, exceto nos casos em que 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).

Como exemplos de coleta de dados sensíveis nos âmbitos público e privado, pode-se citar os formulários a serem preenchidos: no âmbito público, os programas governamentais na área da educação têm como forma de inscrição o preenchimento desses formulários, como é o caso do Exame Nacional do Ensino Médio – ENEM que para efetuar sua inscrição o indivíduo tem que prestar informações consideradas sensíveis, como as de origem racial (GONÇALVEZ; VARELLA, 2018, p. 529).

Já no âmbito privado pode-se citar como exemplo as empresas que tentam extrair esses dados sensíveis através de formulários prontos para candidatura do funcionário ou durante a entrevista de emprego. Essas práticas são feitas com a finalidade de saber previamente se existe algum fator que impeça a contratação, invadindo a esfera privada individual (MACHADO, 2018, p. 198).

Em ambos os casos, sendo preenchidos esses dados, há uma grande responsabilidade por parte do ente público ou privado em armazená-los de forma segura, o que nem sempre acontece. Com isso, 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[...]" (MACHADO, 2018, p. 199).

Do art. 23 até o art. 32 da LGPD, está prevista a regulamentação mais específica de quando o tratamento dos dados pessoais for feito pelo Poder Público. Conforme disciplina Bioni (2019, p. 245), a relação entre o Poder Público e os titulares das informações pessoais é marcada pela desigualdade de poder, uma vez que o ente estatal sempre foi visto como detentor do poder de soberania, tendo o interesse público superioridade hierárquica em relação ao interesse individual. Além disso, o Poder Público, na necessidade de cumprir seus deveres, sempre manteve bancos de dados com informações pessoais coletadas à sua disposição.

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[5] e a LGPD impõe como regra de utilização dessas informações, o dever de atender a finalidade pública, ou seja, com base no interesse público e na execução de competências e atribuições legais do serviço público. Em consonância com o regramento aplicado no âmbito privado, quando o tratamento for feito pelo Poder Público deverá ser observado com rigor a regra de fornecimento de informações claras e contundentes sobre a utilização desses dados, o manuseio dos mesmos e a finalidade da sua aplicação em meios passíveis de acesso público, preferencialmente em sítios eletrônicos (BRASIL, 2018).

Outro ponto a se ressaltar nas mudanças introduzidas pela Lei é o previsto no art. 26, § 1º que apresenta a vedação ao poder público em transferir dados pessoais a que tenha acesso através de banco de dados a entidades privadas, exceto nos casos previstos em que poderá acontecer essa transferência como, por exemplo, em caso de contratos e convênios (IV). Havendo a transferência por essa razão, à autoridade nacional deverá ser comunicada (§ 2º), percebe-se através desses artigos que a mesma desempenhará o papel de fiscalização sobre os atos envolvendo o poder público em relação a disposição desses dados, bem como outros papéis de regulamentação (BRASIL, 2018).

No que diz respeito às sanções previstas no art. 52[6] para caso de descumprimento do previsto na legislação, cabe ressaltar que algumas delas foram vetadas pela Presidência da República, no intuito de adequá-las a realidade da legislação em voga e do contexto social e econômico brasileiro, levando-se em conta a razoabilidade e proporcionalidade, não seguindo tão à risca o previsto no Regulamento Europeu (PINHEIRO, 2018, p. 35).

---

[5] 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.

[6] 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;

As sanções somente serão aplicadas após ser realizado o procedimento administrativo que oportuniza a abertura do prazo para exercer a ampla defesa, e sua aplicação levará em conta a análise do caso concreto para então decidir a forma de aplicação. Essa que poderá ser gradativa, isolada ou cumulativa, seguindo os parâmetros previstos na Lei, como por exemplo, a gravidade e a natureza da infração, se o infrator agiu com boa-fé, se o mesmo teve alguma vantagem com aquele ato, sua condição econômica e possível reincidência, entre outros fatores a serem analisados no caso concreto (BRASIL, 2018).

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

A Autoridade Nacional de Dados Pessoais (ANDP) terá a função de regulamentar e fiscalizar os atos realizados referentes aos dados pessoais seja pela esfera pública ou privada, para que caso necessário tenha que notificar o agente ou até mesmo aplicar multas pelas infrações cometidas. Além disso, está diretamente ligada à Presidência da República, apesar de ser mantida sua autonomia, como sustenta 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, na esfera pública ou 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, pois em outros países já existia esse órgão com poderes autônomos. A ideia dessa autoridade surgiu a partir da Diretiva Europeia de 1995 que instituiu como regra a outros países que compunham a União Europeia o dever de instituí-la também. Seu surgimento foi de tamanha relevância que posteriormente seu modelo foi aplicado em outros países que não eram membros da União Europeia, como por exemplo, Japão e Argentina (MACHADO, 2018, p. 208).

Embora demonstre um caráter inovador e por ser um órgão em funcionamento em outros países, como na Argentina, a Autoridade Nacional ainda deixa dúvidas e receios, principalmente sobre como será realizada a sua atuação prática. Isso implica numa certa insegurança por conta de aparentemente haver uma centralização de poder nas mãos desse órgão que está subordinado à Presidência da República. Porém, por outro lado, visando à 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 da desconformidade com a regra de 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 13.709/18 e sobre a criação da Autoridade Nacional que, inicialmente, passa a ser um órgão integrante da administração pública federal, subordinado à Presidência da República, podendo 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 a de enviar informes com previsão das medidas cabíveis para cessar possíveis violações advindas do tratamento dos dados em poder da Administração Pública, e, ainda, poderá solicitar aos agentes detentores desses dados a publicação de relatórios que contenham informações sobre o impacto referente a 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 especificas referentes a esses dados, entre outros detalhes desse tratamento. Poderá ainda, emitir parecer técnico complementar com o escopo 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 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 que fazem o tratamento das informações pessoais. Além dessas, há outras competências previstas no art. 55-J, que demonstram como se dá sua esfera de atuação e a busca por certas garantias, como no caso do tratamento de dados de idosos, para que seja efetuado da forma mais simplificada e clara

possível, dispondo a eles acessibilidade e estando de acordo com o Estatuto do Idoso (BRASIL, 2019).

Além da Autoridade Nacional, outro agente que surge com a nova Lei de Proteção de Dados é o encarregado, que conforme os ditames da Lei, atuará por indicação do controlador[7], para ser uma espécie de mediador entre as partes interessadas no tratamento dos dados pessoais, ou seja, entre controlador, titular dos dados e a Autoridade Nacional, de forma a manter todos informados sobre o que for necessário (art. 5º, VIII) (BRASIL, 2018).

Por fim, a partir da análise feita da Lei n. 13.709/18, com enfoque voltado para o que é pertinente a Administração Pública, é possível visualizar várias propostas e inovações disciplinadas por ela, levando em consideração sempre 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 manutenção do tratamento dos dados pessoais sensíveis, principalmente no que diz respeito ao Poder Público e como será aplicada essa fiscalização na prática, outrossim, apesar de a ANPD ser um órgão detentor de muitas competências essenciais para efetivar essa proteção, ainda há certo receio quanto à centralização do poder em torno de apenas um órgão.

CONSIDERAÇÕES FINAIS

A nova Lei n. 13.709/18 de proteção de Dados é uma legislação com uma base principiológica e reflete a evolução, no Brasil, de uma longa história de proteção de dados em âmbito mundial, sendo ela uma das mais esperadas leis a entrar em vigor dos últimos tempos, tendo em vista a tardia evolução dessa proteção em território Nacional. Essa Lei foi proposta com base no Regulamento Europeu de Proteção de Dados, que é referência quando se trata desse tema e que foi o principal motivador de sua existência, uma vez que o Brasil chegou a seu limite de postergação de implementação de uma Lei específica sobre proteção de Dados.

Observa-se no decorrer desse estudo que outros países estavam muito à frente do Brasil ao se tratar desse tema, a exemplo a Argentina, que mantém regulamentação especifica 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 à dignidade da pessoa humana, uma vez que para se exercer o efetivo direito à privacidade,

---

[7] 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;

principalmente a informacional, é necessário um posicionamento do Poder Legislativo e Executivo sobre o tema.

Com a implementação dessa nova Lei de Proteção de Dados muitas foram as dúvidas que surgiram, principalmente no que diz respeito à aplicação de suas propostas inovadoras e inéditas, visto que, anteriormente a esta Lei, a proteção de dados era feita por legislações esparsas, dentre elas a Lei n. 12.965/14, conhecida como Marco Civil da Internet, que era aplicada de forma subsidiária para preencher a lacuna da falta de Lei específica. Porém o Marco Civil da Internet não continha essas previsões, nem mesmo regulamentava os dados pessoais sensíveis, que é uma expressão normatizada pela nova Lei.

Além de regulamentar os dados pessoais sensíveis, novidade desta Lei, a Autoridade Nacional, que só existia em outros países, como na Argentina e no Uruguai, e que passou a ser parte do ordenamento jurídico, atuando como órgão da Administração Pública Federal, foi tida como outra previsão impactante. A autoridade nacional foi idealizada com o intuito de ser um órgão autônomo com poderes de regulamentar, fiscalizar e aplicar sanções na esfera privada e pública a fim de fazer valer o que está previsto na Lei. Sua criação foi inicialmente vetada, o que geraria importante lacuna, situação contornada com a edição da Lei n. 13.853/19, que criou e regulamentou a atuação da Autoridade Nacional, atribuindo-lhe diversas competências, dentre elas o poder-dever de zelar pela proteção de dados. Além disso, normatiza como serão aplicadas essas competências e como será composta essa Autoridade, através de conselhos, ouvidorias e outros órgãos que possibilitem a aplicação das normas e regras dispostas na Lei.

Ainda assim, há a preocupação em torno do tratamento dos dados em poder da Administração Pública, que é imprescindível tendo em vista que a Lei de Acesso a informação de certa forma dificulta essa proteção, quando prevê que o interesse público é a regra e o sigilo é a exceção. Apesar de estar de acordo com a LGPD no que se refere a tornar os atos do Poder Público transparentes e acessíveis, pois prevê que sendo feito o tratamento dos dados pelo Poder Público, este deve se te ater as regras de informação, clareza e transparência dos seus atos, a aplicação da LAI pode trazer algumas vulnerabilidades aos dados pessoais.

Embora apresente um regramento que se adequa 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 e amoldada conforme a necessidade e interesse social e que os mecanismos de fiscalização da Autoridade Nacional serão eficazes para inibir possíveis violações a esses dados. Outro fator que é levado em consideração quando o assunto são dúvidas e inseguranças é a centralização do poder em torno da Autoridade Nacional, principalmente pelo fato desta, inicialmente, ter ligação e subordinação direta a Presidência República, o que faz com que uma das maiores preocupações seja em relação ao desvio de finalidade deste órgão.

Apesar de haver dúvidas e receios quanto a algumas previsões dessa Lei, ela é uma grande conquista para a legislação brasileira, principalmente para o âmbito privado. Com efeito, da análise da LGPD permite pressupor que ela cumprirá muito mais seu papel protetivo dos direitos dos cidadãos na esfera privada o que demonstra que ainda há muito para se avançar no que diz respeito à proteção de dados pessoais na 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.