DOI 10.5433/24157-108104-1.2023v18n2p.169

A PROTEÇÃO DOS DIREITOS DE PERSONALIDADE PELO PODER PÚBLICO: UM ESTUDO SOBRE A RESPONSABILIDADE DO ESTADO NO TRATAMENTO DE DADOS PESSOAS

THE PROTECTION OF PERSONALITY RIGHTS BY THE PUBLIC GOVERNMENT: A STUDY ON THE STATE'S RESPONSIBILITY IN PROCESSING PERSONAL DATA

Rodrigo Róger Saldanha*
José Sebastião de Oliveira**

Como citar: SALDANHA, Rodrigo Róger; OLIVEIRA, José Sebastião de. A proteção dos direitos de personalidade pelo poder público: um estudo sobre a responsabilidade do Estado no tratamento de dados pessoais. **Revista do Direito Público**, Londrina, v. 18, n. 2, p. 169-186, ago.2023. DOI 10.5433/24157-108104-1.2023v18n2p.169. ISSN: 1980-511X

Resumo: No cenário digital, o advento da tutela dos dados pessoais no ordenamento jurídico pátrio, através da Lei Geral de Proteção de Dados, representa grande avanço. Sem prejuízo de sua importância para a evolução tecnológica, social e econômica, o mau uso dos dados pessoais pode estimular discriminações, causando prejuízos ao livre desenvolvimento da personalidade, mesmo assegurada a autodeterminação informativa, ferindo garantias constitucionais, especialmente quando manejados pelo Poder Público. Valendo-se da metodologia hipotético- dedutiva, a presente pesquisa tem por objetivo apontar o reconhecimento de um direito fundamental autônomo de proteção aos dados pessoais, distinto do direito à privacidade, bem como propor reflexão acerca dos impactos do tratamento de dados pela administração pública, partindo da análise de pontos pertinentes da lei, relacionados à autonomia do órgão fiscalizador, garantindo a observância rigorosa da transparência e finalidade, constatando-se, por fim, que em vista do domínio dos dados, há a intensificação da vigilância estatal, fragilizando instituições democráticas.

Palavras-chave: LGPD; discriminação; autoridade nacional de proteção de dados.

Abstract: In the digital scenario, the advent of the protection of personal data in the national legal system, through the

*Doutorando em Direito pelo Centro Universitário de Maringá (2019-2023), Bolsista PROSUP/ CAPES pelo Programa de Pós-Graduação, sob orientação do Dr. José Sebastião de Oliveira. Participante discente do grupo de pesquisa Reconhecimento e garantia dos direitos da personalidade, sob a liderança da Dr. Valéria Silva Galdino Cardin (2019-2023). Mestre em Ciências Jurídicas pelo Centro Universitário de Maringá / Bolsista CAPES (2015-2017). Especialista em Educação Ambiental pela Universidade Federal de Santa Maria - UFSM (2014-2015). Especialista em Ciências Penais pela Universidade Estadual de Maringá - UEM (2012 - 2013). Graduação em Direito pela Faculdade Metropolitana de Maringá - Bolsa PROUNI (2007-2011). Professor de Direito da Pontifícia Universidade Católica do Estado do Paraná – PUC/PR. currículo lattes: http://lattes.cnpq.br/8968070508046566. Orcid: https://orcid.org/0000-0001-5329-2316. Contato: saldanhadoc@gmail.com

**Pós-doutorado em Direito pela Universidade de Lisboa (2013). doutorado em Direito pela Pontifícia Universidade Católica de São Paulo (1999). Mestrado em Direito Negocial pela Universidade Estadual de Londrina (1984). Graduação em Direito pela Universidade Estadual de Direito de Maringá (1973). Atualmente é professor da graduação e Pós-Graduação Stricto Sensu (mestrado e Doutorado) do Centro Universitário de Maringá (UNICESUMAR). Participante docente do grupo de pesquisa Reconhecimento e garantia dos direitos da personalidade. Membro do Conselho Nacional de Pesquisa e Pós-Graduação em Direito, sociedade científica do Direito no Brasil. Tem experiência na área do Direito, com ênfase em Direito Civil, atuando principalmente nos seguintes temas: direitos da personalidade, família, sucessões, responsabilidade civil e, também em metodologia do ensino jurídico. currículo lattes: http://lattes.cnpq.br/7878157645842709. Orcid: https://orcid.org/0000-0001-9429-3841 Contato: drjso1945@gmail.com

General Data Protection Law, represents a major advance. Without prejudice to its importance for technological, social, and economic evolution, the misuse of personal data can stimulate discrimination, causing damage to the free development of personality, even though informational self-determination is ensured, hurting constitutional guarantees, especially when handled by Government. Drawing on the hypothetical-deductive methodology, this research aims to point out the recognition of an autonomous public right to protection personal data, distinct from the right to privacy, as well as propose reflection on the impacts of data processing by the public administration, based on the analysis to relevant points of the law, related to the autonomy of the supervisory body, ensuring strict compliance with transparency and purpose, noting, finally, that the view of the domain of personal data, there is the intensification of state surveillance, weaking democratic institutions.

Keywords: general data protection law; discrimination; national data protection authority.

INTRODUÇÃO

A datificação da vida humana é perceptível e a Lei Geral de Proteção de Dados (LGPD) consagrou a expressão genérica "tratamento de dados" para se referir às diversas operações, como coleta, produção, armazenagem, avaliação e transferência, que envolvem dados pessoais, inerentes à grande maioria das atividades desempenhadas socialmente. A criação da LGPD se deu ante a necessidade de inovação do ordenamento jurídico para acompanhar as transformações sociais, visando efetivar proteção aos titulares, mas sem restringir o desenvolvimento socioeconômico, que possui os dados pessoais como referencial.

O Poder Público, por sua vez, possui grande monopólio sobre as informações dos cidadãos, e apesar de possibilitar o progresso e aperfeiçoamento da atuação estatal, o uso de dados não está a salvo de situações indesejadas, podendo acentuar condição de vigilância, sendo por este ângulo que se pretende refletir acerca dos impactos da LGPD. Ainda, espera-se distinguir a proteção de dados pessoais das demais garantias constitucionais, apontando a existência de um direito fundamental autônomo e independente da privacidade.

Em primeiro momento, contextualiza-se a sociedade da informação e o alcance jurídico trazido pela LGPD, asseverando a proeminência da autodeterminação informativa frente às decisões automatizadas. Em seguida, adentra-se ao debate acerca do caráter fundamental conferido a tutela dos dados pessoais. Após, a pesquisa se dedica à análise de algumas nuances da aplicação da lei ao tratamento de dados pelo Poder Público, sobretudo pela facilitação de coleta de informações, e a necessidade de independência da autoridade fiscalizadora. Por fim, reflete sobre o aumento do monitoramento dos cidadãos, justificado pelo contexto pandêmico, e a relevância da proteção dos dados para manutenção hígida da democracia.

A justificativa do estudo se dá, em razão da expressiva influência dos dados pessoais, sendo inegável que os cidadãos são vulneráveis na relação com o Poder Público, possuidor da maioria das bases de dados. Agrava-se ao fato de que cenários emergenciais costumam propiciar a relativização de direitos, alegadamente em prol do interesse público, pelo que se vislumbra a necessidade de abordar a controvérsia da proteção de dados como direito fundamental, e analisar riscos que a atuação desenfreada da administração pública pode gerar para a sociedade, seja aos indivíduos e a própria coletividade.

1 A AUTODETERMINAÇÃO INFORMATIVA E NOVOS DIREITOS

Mudanças disruptivas e irreversíveis surgiram na sociedade, em função da internet. As inúmeras inovações tecnológicas, como os dispositivos móveis, a nanotecnologia, a inteligência artificial (*IA*) e a internet das coisas (*IoT*), dentre outras, exercem um papel fundamental no desenvolvimento da humanidade em um mundo cada vez mais volátil, interligado por um meio digital onipresente e em constante observação.

Aliado às tecnologias, o fluxo massivo de informações, decorrente do avanço dos meios de comunicação e interação social, influencia diretamente o desenvolvimento socioeconômico, haja vista que "os dados pessoais dos cidadãos se converteram em um fator vital para a engrenagem da economia da informação" (BIONI, 2020, p. 12), tornando possível, *e.g.*, a identificação de padrões de consumo e o reconhecimento de demandas sociais. Infere-se, desde logo, que o controle e a eficiência são o que fundamenta o uso de dados pessoais (DONEDA, 2020, p. 33).

A sociedade contemporânea, então, vive a chamada "era digital", cujo traço marcante é o protagonismo do mundo *online*, de modo que os indivíduos, enquanto conectados, fornecem uma infinidade de dados sobre suas vidas, convicções, preferências, e até mesmo suas condições emocionais, criando verdadeiros rastros virtuais, sendo admissível dizer que o ser humano se tornou multifacetário.

No que diz respeito à virtualização da pessoa, Humberto Nogueira Alcalá aponta que:

> Neste cenário, o cidadão, nos seus mais diversos papéis sociais – como contribuinte, paciente, trabalhador, beneficiário de programas sociais ou como consumidor – tem seus dados processados diuturnamente. Uma combinação de técnicas automatizadas permite a obtenção de informações sensíveis sobre os cidadãos e a construção de verdadeiros perfis virtuais, que passam a fundamentar a tomada de decisões econômicas, políticas e sociais, criando uma demanda por instrumentos capazes de contrabalancear possíveis abusos (apud MENDES; DONEDA, 2016, p. 449).

No entendimento de Doneda (2020, p. 8), o dado representa uma "pré-informação", a qual precisa ser interpretada[6]. Esta abundância de "pré-informações" é armazenada em banco de dados e processada por mecanismos de Tecnologia da Informação (TI), como o *Big Data*, traduzindo dados desconexos em conhecimento, com determinada finalidade. A abrangência da norma jurídica pode ser dimensionada por meio da conceituação de dados pessoais, uma vez que "não seria qualquer dado que teria repercussão jurídica, mas, somente, aquele que atraísse o qualificador pessoal." (BIONI, 2020, p. 59).

Nesse contexto, conforme estabelecido no Art. 5º, inc. I, da LGPD, dado pessoal é toda "informação relacionada a pessoa natural identificada ou identificável" (BRASIL, 2018a), portanto, para saber se determinado dado recebe tutela jurisdicional, torna-se necessária a "análise contextual que depende de qual tipo de informação poder ser extraída de uma base de dados" (BIONI, 2015, p. 18), Frente ao exposto, um dado pessoal pode ser, a título exemplificativo, desde o nome até a localização geográfica da pessoa natural.

Por sua vez, aos dados pessoais sensíveis, conceituados pelo Art. 5º, inc. II, da LGPD[1], é assegurada proteção mais elevada, uma vez que "a técnica de mineração de dados constitui uma tecnologia potencialmente discriminatória" (MENDES, 2014, p. 110), deste modo, colocando o titular de dados sensíveis em maior vulnerabilidade.

1 Conforme o Art. 5, inc. II, da LGPD: "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" (BRASIL, 2018a).

O parágrafo 2º, do Art. 12, da LGPD estabelece que "podem ser considerados dados pessoais, aqueles utilizados para formação de perfil comportamental de pessoa natural, se identificada" (BRASIL, 2018a), nesse cenário, é válido salientar que atualmente, diversas técnicas, como o *profiling* ou *grouping*[2] e a tomada de decisões automatizadas, influenciam no livre desenvolvimento da personalidade, bem como no reconhecimento da identidade pessoal nos meios sociais, real e virtual.

No entanto, os sistemas automatizados se utilizam de algoritmos, os quais podem "confirmar e naturalizar preconceitos, a depender de quais sejam seus inputs e de como os processarão" (CALABRICH, 2020, p. 11). Repercutindo na coletividade, e não apenas no âmbito individual, de modo que:

> [...] passa-se a considerar também os abusos decorrentes do tratamento dos dados pessoais como um problema de igualdade, sempre que sua inadequada utilização acarretar ações potencialmente discriminatórias. Exemplo disso é a discriminação racial realizada com base em dados pessoais, também denominada de *racial profiling*, em que bancos de dados com perfis étnicos ou raciais são utilizados para fundamentar determinadas decisões (MENDES; DONEDA, 2016, p. 5).

Visando coibir mencionados abusos na utilização de dados, é que a LGPD consagrou a autodeterminação informativa como um de seus fundamentos basilares, pelo qual se assegura o direito, ao titular, de supervisionar o uso de seus dados pessoais, podendo obter do controlador, o acesso, a correção ou exclusão de dados, entre outras ações, consoante ao Art. 18, da LGPD[3]. No entanto, sua a efetividade vincula-se ao princípio da transparência, haja vista ser necessária a ciência plena do titular para o exercício efetivo de controle do fluxo informacional a seu respeito.

Assim, permitir a coleta e o tratamento desregulado de dados pessoais, sem que houvesse balizas jurídicas conferindo mecanismos protetivos, significaria prejudicar a formação da personalidade do indivíduo e o modo como seria exposto para a sociedade, ferindo direitos e fomentando discriminações. No entanto, a legislação brasileira não era satisfatória acerca do tema, embora leis setoriais[4] pincelassem alguma proteção aos dados pessoais.

2 Sobre perfilação: "[...] um perfil de um grupo ou indivíduo é criado a partir do cruzamento de uma grande quantidade de dados disponíveis e uma vez estabelecido um perfil o sujeito será avaliado com base nele. É como se a resposta já estivesse dada e a única variável seria a pergunta. Os riscos dessa mudança para o desenvolvimento da identidade e para o exercício da autonomia são grandes, pois o indivíduo tem pouco (ou nenhum) controle sobre como é 'visto'." (MARTINS; HOSNI, 2019, p. 46-54).

3 Conforme Art. 18, da LGPD: "O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição: I - confirmação da existência de tratamento; II - acesso aos dados; III - correção de dados incompletos, inexatos ou desatualizados; IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei; V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial; VI - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei; VII - informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados; VIII - informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa; IX - revogação do consentimento, nos termos do § 5º do art. 8º desta Lei" (BRASIL, 2018a).

4 No Brasil, até o ano de 2018, leis esparsas regulavam a proteção aos dados pessoais, tais como: o Código de Defesa do Consumidor (CDC – Lei nº 8.078/1990); a Lei de Cadastro Positivos (Lei nº 12.414/2011); a Lei de Acesso à Informação (Lei nº 12.527/2011); o Marco Civil da Internet (Lei nº 12.965/2014); e a Política de Dados Abertos – PDA (Dec. nº 8.777/2016).

Somando-se à vigência, a partir de maio de 2018, do regulamento europeu de proteção aos dados, o *General Data Protection Regulation* (GDPR), fez-se necessária a adaptação do ordenamento jurídico para harmonizar as normas pré-existentes e tutelar interesses distintos, em prol do desenvolvimento, bem como para assegurar proteção aos titulares. Assim, em 14 de agosto de 2018, foi promulgada a Lei nº 13.709, então, denominada como Lei Geral de Proteção de Dados Pessoais, representando uma tutela específica e homogênea ao tratamento dos dados pessoais e sensíveis, no Brasil.

2 DADOS PESSOAIS, UM NOVO DIREITO?

Da análise doutrinária e jurisprudencial, se observa claramente o delinear do reconhecimento de um novo direito fundamental autônomo e, garantido constitucionalmente, voltado à proteção de dados. Nesse sentido, surgiu o Projeto de Emenda à Constituição (PEC) nº 17, de 2019, com a pretensão de inserir "a proteção de dados pessoais, inclusive nos meios digitais", ao rol do Art. 5º, da Constituição da República Federativa do Brasil, de 1988 (CRFB/88). Mais recentemente, e deixando diversos pesquisadores perplexos pela urgência da tramitação temática, foi promulgada em fevereiro de 2022 a Emenda Constitucional n. 115/2022, que elenca a proteção de dados pessoais como um direito fundamental.

No entanto, tal reconhecimento se transformou em um debate bastante controverso, posto que parte da doutrina entende a tutela de dados pessoais somente como desdobramento do direito à privacidade, intimidade e inviolabilidade das telecomunicações. Por outro lado, aqueles favoráveis ao reconhecimento desse direito fundamental defendem que "não existem mais dados irrelevantes diante do processamento eletrônico e ubíquo de dados na sociedade da informação." (MENDES; DONEDA 2018, p. 555-587).

Com efeito, esta tutela jurídica abarca qualquer tipo de dados pessoais, seja aqueles que se encontram na esfera pública ou na esfera privada (BIONI, 2020, p. 94).

As demais tutelas garantidas constitucionalmente como proteção à privacidade e à intimidade objetivam proteger aspectos da vida privada, honra e imagem do cidadão, da interferência indesejada de terceiros (do Estado ou de particulares), tratando-se de liberdade de abstenção individual, enquanto a tutela de dados pessoais se mostra mais ampla.

Ora, o fornecimento de qualquer tipo de dados é massivo e diário. As pessoas compartilham de sua privacidade, demasiadamente, nas inúmeras mídias sociais, aplicativos de relacionamentos, *YouTube*, entre outros, sendo certo que as informações da vida privada são exibidas publicamente. Entretanto, não se perde de vista que muitas informações pessoais não são expostas ao público, porém, encontram-se armazenadas na rede, *e.g.*, conteúdo de mensagens e *e-mails*, imagens diversas, dados bancários, dados de saúde, todos, suscetíveis de invasão e vazamento.

Evidencia-se, portanto, que os dados públicos e privados são espécies de uma categoria maior, qual seja, a dos dados pessoais, cuja proteção foi, indubitavelmente, conferida no texto

dado à LGPD, considerando que o tratamento e a segurança de tais dados são imprescindíveis.

Além disso, a LGPD consagrou faculdades jurídicas e diretrizes próprias, que se diferem da forma de aplicação dos demais direitos fundamentais, considerando que "a regulamentação da proteção de dados pessoais é uma legislação principiológica." (PINHEIRO, 2020, p. 40).

De fato, a referida lei é repleta de princípios que exprimem valores próprios e essenciais para a sua compreensão e efetivação, e é por conta desta autonomia, também, que se atribui natureza de direito fundamental a proteção de dados.

Em consonância:

> [...] o direito à proteção de dados pessoais reclama uma normatização própria que não pode ser reduzida a uma mera "evolução" do direito à privacidade, mas encarada como um novo direito da personalidade que percorre, dentre as outras liberdades e garantias fundamentais, a liberdade de expressão, de acesso à informação e de não discriminação. Em última análise, trata-se da nossa própria capacidade de autodeterminação (BIONI, 2020, p. 95).

No que tange à jurisprudência, o Supremo Tribunal Federal (STF), recentemente, proferiu considerável decisão acerca do tema[5], ao referendar liminar que suspendeu a eficácia da Medida Provisória (MPV) nº 954/2020 (BRASIL, 2020b), a qual estabelecia o compartilhamento de dados (nomes, números de telefone e endereços) por empresas de telecomunicação à Fundação Instituto Brasileiro de Geografia e Estatística (IBGE), visando a produção de estatística oficial, durante a emergência de saúde pública causada pelo novo Coronavírus (Covid-19), posto que atribuiu a natureza de garantia constitucional a esta tutela e analisou a eficácia da MPV, por meio de diretrizes da CRFB/88 e da própria LGPD.

Na ótica de Laura Schertel Mendes e Gabriel Campos Soares da Fonseca (2020, p. 15):

> O Tribunal formulou, assim, uma tutela constitucional mais ampla e abstrata do que o direito à inviolabilidade da esfera íntima e da vida privada. Essa tutela poderá ser aplicada em inúmeros casos futuros envolvendo a coleta, o processamento e o compartilhamento de dados pessoais no Brasil. O conteúdo desse direito fundamental exorbita aquele protegido pelo direito à privacidade, pois não se limita apenas aos dados **íntimos** ou privados, ao revés, refere-se a qualquer dado que identifique ou possa identificar um indivíduo.

Destarte, é possível interpretar a referida decisão do STF de forma favorável ao reconhecimento de direito fundamental a proteção de dados, alinhado ao posicionamento atual e majoritário de juristas, sendo certo que a proposta da MPV em questão, demonstra uma forma de

5 Em decisão monocrática, a ministra Rosa Weber deferiu medidas cautelares em cinco ações diretas de inconstitucionalidade, em julgamento conjunto (ADIs 6387, 6388, 6389, 6390 e 6393), posteriormente referendadas, por maioria, pelo plenário do STF. A ministra determinou que o IBGE se abstenha de requerer os dados de operadoras de telefonia, por não vislumbrar interesse público legítimo no compartilhamento de dados, uma vez que MPV nº 954/2020 não é clara acerca da finalidade específica e o modo de utilização, tampouco dispõe sobre mecanismos e procedimentos de segurança, contrariando a efetiva proteção à direitos fundamentais.

utilização dos dados pessoais pelo Poder Público visando aperfeiçoar políticas públicas, tendo em vista, o contexto pandêmico.

3 INTERESSE SOCIAL VIGILÂNCIA E NOVAS PERSPECTIVAS DO ESTADO

É notório que operações envolvendo dados por parte da Administração Pública não tiveram início por conta da crise de saúde pública atualmente vivenciada, considerando que os "órgãos do Poder Público são controladores de quantidade maciça de dados pessoais, não apenas para a execução de políticas públicas, mas também em decorrência de suas respectivas atividades." (SCOPEL, 2020, p. 56).

Menciona-se, exemplificativamente, as bases de dados da Receita Federal, do Sistema Único de Saúde (SUS), do Sistema Nacional de Educação (SNE), de aplicativos como "Coronavírus – SUS", "Caixa Tem", de programas de assistência social como Bolsa Família, e até os censos elaborados pelo IBGE, entre outras. Determinou-se, por conseguinte, que LGPD também é aplicável às pessoas jurídicas de direito público[6]

Hodiernamente, o desenvolvimento social, encontra-se profundamente vinculado ao processamento de dados dos cidadãos pelos órgãos públicos, inclusive, sendo vistos como ferramentas altamente relevantes para formulação e aperfeiçoamento de políticas públicas, que funcionam como "vocalizador de demandas" (GONÇALVES, 2019, p. 22), cunhando o conceito de *smart cities*:

> As cidades inteligentes dispõem de uma quantidade massiva de dados estruturados, dos quais, por meio do processamento de algoritmos do tipo *machine learning*, são extraídas informações úteis visando conferir soluções para melhorias nas áreas social, econômica, ecológica e de infraestrutura das cidades. Para tanto, as cidades inteligentes se valem do *big data*, alavancado pela internet das coisas, para elevar o padrão dos cidadãos, trazendo maior eficiência nos serviços públicos (ABRUSIO, 2020. p. 5-17).

No entanto, muito embora o poderio dos dados pessoais e das particularidades normativas impostas à administração pública, a segurança do tratamento é questionável em diversos aspectos, por isso, sem pretensão de exaurir a matéria dada a abrangência das normas trazidas pela nova lei, o presente estudo visa analisar pontos pertinentes à reflexão sobre os impactos de referido domínio dos dados, pelo Poder Público.

6 De acordo com o Art. 23, da LGPD, especificamente àquelas referidas no parágrafo único do Art. 1º da Lei de Acesso à Informação (Lei nº 12.527/11): "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". (BRASIL, 2011).

3.1 Transparência e finalidade

A atuação do Poder Público deve vislumbrar a base principiológica na proteção dos dados, e; como dito anteriormente, a autodeterminação informativa é um dos pilares fundamentais desta proteção, assegurando aos titulares o direito de controlar o uso de seus próprios dados pessoais. Nessa seara, o consentimento, torna-se uma das principais formas de efetivar esse direito, e consiste na "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada" (BRASIL, 2018a), conforme disposto no Art. 5º, inc. XII da LGPD.

Contudo, as hipóteses de dispensa do consentimento são mais abrangentes quando se fala em tratamento ou compartilhamento de dados em favor do interesse público[7], de modo que "as exceções inseridas para o setor acabam dando margem a uma interpretação extensiva da lei e abarcando um número considerável de situações" (GONÇALVES, 2019, p. 22), trazendo inseguranças jurídicas acerca do manejo dos dados dos cidadãos. Por outro lado, visando contrabalancear a facilitação de acesso, ao Poder Público é imposta a observância mais rigorosa dos princípios da finalidade e da transparência.

Até mesmo nos casos em que o consentimento não é exigido, a Administração Pública deve estabelecer sistemas de gestão de dados que possam assegurar a transparência, uma vez que esta é a principal diretriz da lei protetiva de dados (PINHEIRO, 2019). O tratamento, então, deve ser precedido de publicidade clara e atualizada, em veículos de fácil acesso pelos titulares, sobre a finalidade específica, os procedimentos e a forma de uso dos dados coletados.

De acordo com o princípio da finalidade, o tratamento de dados deve ser realizado para "propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível", e especificamente quanto a atuação do Poder Público, a motivação será, em última análise, o atendimento ao interesse público, visando "executar as competências legais ou cumprir as atribuições legais do serviço público"[8].

A efetividade prática das disposições legais, ou *enforcement* da lei, no entanto, depende da atuação da Autoridade Nacional de Proteção de Dados (ANPD), uma vez que a "a existência desses órgãos é essencial para a implementação da legislação e da cultura da privacidade no país" (MENDES, 2014, p. 49), a quem cabe zelar pela proteção dos dados pessoais, implementar e fiscalizar o uso de dados, aplicar sanções em caso de inobservância, e orientar a interpretação da lei, dentre outras competências relacionadas no Art. 55-J, da LGPD.

3.2 Autonomia da autoridade nacional de proteção de dados

A principal preocupação em torno da ANPD diz respeito à sua autonomia, característica essencial ao exercício das funções atribuídas ao órgão, na garantia do direito à proteção de dados.

7 Dispostas nos Artigos 11, 26 e 27, da Lei Geral de Proteção de Dados.
8 Art. 6º, I e Art. 23, da LGPD.

Isso porque, embora tenha sido estruturada recentemente pelo Decreto nº 10.474, de 26 agosto de 2020, a autoridade vincula-se à administração pública direta e seus membros devem ser escolhidos por livre nomeação da Presidência da República, fator que causa desconfiança acerca da independência da ANPD.

Estudo realizado pelo Instituto Brasileiro de Defesa do Consumidor (IDEC), a partir da análise de modelos das autoridades de proteção dos dados vigentes em países da América Latina, com o intuito de investigar se a efetividade dos órgãos se relaciona com o grau de independência, aponta, em tese, que considerando a vinculação direta com o Poder Executivo, há possibilidade de conflito de interesses, de modo que as decisões, que devem ser técnicas, podem vir a ser tomadas por influência política, até mesmo ante o temor de retaliações; e que a ausência de oposição "influencia a eficácia e dificulta a concretização da independência enquanto órgão fiscalizador." (SIMÃO, 2019, p. 36-37).

Sobre a autoridade brasileira, a referida pesquisa conclui que:

> A Autoridade Nacional de Proteção de Dados Pessoais brasileira corre o risco de, em decorrência da edição da Medida Provisória nº 869/2018 e de sua votação no Congresso, estar administrativamente vinculada à Presidência da República. As experiências estudadas na pesquisa em questão, no entanto, revelam que este não seria um bom desenho institucional para o órgão. [...] Por outro lado, o melhor modelo é aquele cuja autoridade possua personalidade jurídica própria, estando desvinculada da administração direta, e a nomeação de seus membros passem pelo crivo da oposição, como no Congresso, ou admita a participação da sociedade civil nesta escolha (BRASIL, 2018b).

A solução apresentada pelo estudo se alinha ao posicionamento de estudiosos sobre o modelo de constituição da ANPD, a qual possui natureza jurídica transitória, podendo se tornar entidade da administração pública federal indireta, sob o regime de autarquia especial, respaldando-se no Art. 55-A, §1º, da LGPD: "Os agentes públicos vinculados à Autoridade, obrigatoriamente, terão o dever de obediência ao órgão superior, já que há vínculo hierárquico com a Presidência da República" (GONÇALVES, 2019, p. 117) logo, mencionada desvinculação importaria em maior confiança na autonomia da autoridade para aplicação de políticas de proteção dos dados, fortalecendo a atuação do órgão, inclusive frente aos Poder Executivo:

> Autonomia técnica não é o mesmo que autonomia (ou independência) funcional. Sendo órgão da administração pública federal subordinado à Presidência da República, não é desprezível a possibilidade de ingerência indevida sobre questões que, a rigor, deveriam ser estritamente técnicas. [...] Assim, o problema se amplia quando for o próprio Estado-Administração aquele contra quem pese a suspeita de tomar uma decisão automatizada ilicitamente discriminatória. O ideal é que seja transformada o quanto antes em entidade da administração pública federal indireta, submetida a regime autárquico especial, como prevê o § 1º do art. 55-A (CALABRICH, 2020, p. 12).

A avaliação concreta dos desdobramentos da estruturação da ANPD, da forma como se deu, depende de análise futura por se tratar de recente inovação no ordenamento jurídico, porém, mencionada pesquisa possibilita a percepção de que a legislação protetiva de dados ainda está em fase de implementação, no Brasil, apesar de a Lei Geral de Proteção de Dados representar grande marco jurídico para o tema, sendo certo que os dados pessoais dos cidadãos não estão resguardados de eventuais incidentes e riscos.

3.3 Vigilância social e democracia

A sociedade da informação está acompanhada, *pari passu*, de ininterrupta vigilância, embora isto não seja tão evidente, considerando a dispersão do monitoramento, em razão do avanço das tecnologias, ou seja, "ao navegar pela internet ou utilizar serviços proporcionados pela rede, o internauta atua tranquilamente, sem perceber em concreto como está sendo monitorado, por quem e com que finalidade." (GUARDIA, 2020, p. 494).

Além da constante vigilância já empenhada pelo Poder Público, os dados pessoais dos cidadãos entraram em foco no cenário de pandemia causado pelo vírus *SARS-CoV-2*, como forma de auxiliar a contenção da doença e o respeito às determinações de quarentena, isolamento e distanciamento social, posto que "é justamente pela sua posição central na organização social e pela capacidade de serem utilizados como insumo para que se alcance o interesse público, que se legitima o uso dos dados pessoais pelas autoridades estatais (KITAYAMA, 2020, p. 35-42).

Embora suspensa a eficácia da MPV nº 954/2020, pelo STF, o compartilhamento de dados pessoais como forma de enfrentamento da Covid-19, se instaurou, tendo em vista que o Art. 6º da Lei nº 13.979, de 2020[9] criou a obrigatoriedade do compartilhamento de dados essenciais "à identificação de pessoas infectadas ou com suspeita de infecção pelo coronavírus", sob argumento de evitar a propagação do vírus, medida largamente questionada, em vista da ambiguidade redacional da lei, porque é possível interpretar "dados essenciais" como dados pessoais e/ou dados anonimizados, dando margem para abusos e para o uso indevido de dados, sem o controle do titular, em contrariedade às diretrizes trazidas pela LGPD.

A finalidade específica e a segurança de armazenagem dos dados compartilhados também merecem atenção, ante a superficialidade da lei. Menciona-se objetivo genérico de "evitar a propagação do vírus", mas não determina a forma como os dados serão tratados para tal fim. Além disso, estabelece a garantia de "sigilo das informações", sem apontar qualquer mecanismo de proteção aos dados coletados, tal qual estabelecido pelo Art. 46, da LGPD.[10]

9 Conforme o Art. 6º: É obrigatório o compartilhamento entre órgãos e entidades da administração pública federal, estadual, distrital e municipal de dados essenciais à identificação de pessoas infectadas ou com suspeita de infecção pelo coronavírus, com a finalidade exclusiva de evitar a sua propagação. § 1º A obrigação a que se refere o caput deste artigo estende-se às pessoas jurídicas de direito privado quando os dados forem solicitados por autoridade sanitária. § 2º O Ministério da Saúde manterá dados públicos e atualizados sobre os casos confirmados, suspeitos e em investigação, relativos à situação de emergência pública sanitária, resguardando o direito ao sigilo das informações pessoais (BRASIL, 2020a).

10 De acordo com o estabelecido no Art. 46, da LGPD: Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito (BRASIL, 2018a).

O destino das informações também é incerto, levando em conta que a lei é omissa sobre a eliminação ou exclusão dos dados após o tratamento, ou sobre a forma como serão operados, ou seja, não há garantias legais ou até mesmo confiança na boa-fé dos órgãos públicos de que os dados pessoais serão descartados após o período pandêmico. A descredibilidade nas ações do governo aliada à inadvertência legal indica que referidos bancos de dados podem ser aperfeiçoados e mantidos para fins de vigilância e controle (BARROS, 2020, p. 35-42).

Garcia aborda a problemática, concluindo que se a pretensão da lei for:

> [...] a identificação do indivíduo contagiado, a obrigação de entidades públicas e privadas de comunicar obrigatoriamente (Artigo 6º, §1º) certamente levanta preocupações de vigilância social mais profundas, tendo em vista que permitiria às autoridades públicas colherem dados pessoais e pessoais sensíveis de virtualmente toda a população brasileira por meio de via transversa, na qual não haveria a efetiva possibilidade do titular de dados de exercer os seus direitos e se opor à transferência [...] **É fundamental que a vigilância epidemiológica – natural e necessária numa sociedade democrática – não seja fundamento de vigilância social. Não é distópico imaginar um cenário no qual o governo coleta informações extremamente** invasivas sob subterfúgios de administração da saúde, mas utiliza os dados para propósitos diversos (GARCIA, 2020, p. 113-121).

Ocorre que a intensificação da vigilância em cenários emergenciais, nos quais a sociedade se encontra vulnerável, ansiando por soluções vindas do Poder Público, importa em riscos para os cidadãos e para as instituições democráticas, pois viabiliza a chancela de medidas abusivas, que podem ser usadas para finalidades distintas daquelas que às autorizaram, com a relativização de garantias constitucionais. A ministra Rosa Weber frisou justamente este ponto no julgamento das Ações Diretas de Inconstitucionalidade (ADIs) propostas contra a Medida Provisória nº 954/2020[11].

Não se pode olvidar que, atualmente, no ordenamento jurídico brasileiro, coexistem a Lei Geral de Proteção de Dados, evidenciando "seriedade e importância do país na proteção das liberdades, de modo a servir como instrumento a permear relações mais transparentes e menos abusivas" (SILVA, 2019, p. 94-122), e os Decreto nº 10.046 e Decreto nº 10.047, instituindo o Cadastro Base do Cidadão e o Cadastro Nacional de Informações Sociais, que englobam desde números de documentos até "atributos biométricos, biográficos e genéticos" dos brasileiros, com a aparente finalidade de aprimoramento das políticas públicas e criação de meio unificado para identificação do cidadão. Indubitavelmente, a maioria dos dados pessoais dos cidadãos brasileiros vão constar de referidos cadastros.

A tutela de dados pessoais é essencial para a manutenção da estrutura social e da vida comunitária (LEONARDI, 2011, p. 122), sendo certo que o acesso irrestrito e o amplo domínio das informações pelos órgãos e entidades da administração pública representam riscos nefastos. Além

11 Não se subestima a gravidade do cenário de urgência decorrente da crise sanitária nem a necessidade de formulação de políticas públicas que demandam dados específicos para o desenho dos diversos quadros de enfrentamento. O seu combate, todavia, não pode legitimar o atropelo de garantias fundamentais consagradas na Constituição (BRASIL, 2020, p. 12).

do mais, operacionalizar dados sensíveis, potencialmente discriminatórios, em contrariedade às normas da LGPD no que tange à transparência e segurança dos dados, gera desconfiança nas ações governamentais. No que se refere ao controle exercido pelo Estado mediante a detenção de dados, Doneda (2020, p. 34), leciona que:

> [...] um pressuposto para uma administração pública eficiente é o conhecimento tão acurado quanto possível da população [...], o que implica, por exemplo, a realização de censos e pesquisas e o estabelecimento de regras para tornar compulsória a comunicação de determinadas informações pessoais à administração pública. Em relação ao controle, basta acenar às várias formas de controle social que podem ser desempenhadas pelo Estado e que seriam potencializadas com a maior disponibilidade de informações sobre os cidadãos, aumentando seu poder sobre os indivíduos - não é por outro motivo que um forte controle da informação é característica comum aos regimes totalitários.

Costumeiramente, os órgãos da Administração Pública, se utilizam do *profiling* por meio de decisões automatizadas, cujas técnicas são potencialmente discriminatórias, como explanado alhures, seja para categorizar cidadãos, seja para o impulsionamento de campanhas políticas. Certo é, que as práticas apontadas influenciam na capacidade de formar senso crítico e conscientização, bem como na autonomia e no livre desenvolvimento da personalidade como ser político.

Com efeito, a intensificação da vigilância e o aumento do poder estatal por meio do controle de dados dos indivíduos é característica de Estados marcados por autoritarismo, ao reverso daqueles constituídos como Estado Democrático de Direito, nos quais se pressupõe garantia de direitos fundamentais e de pluralismo, de modo que as opiniões públicas são "os elementos direcionadores de políticas e ações governamentais" (RANIERI, 2013, p. 317).

Boehme-Neßler (2016, p. 228) propõe rica reflexão sobre autonomia e manutenção da democracia:

> Free minds are a foundation of free societies. No wonder, that the secret ballot is an important tool of democratic elections ¾ and the symbol of democracy. It makes sure people can vote free and autonomously without being observed, coerced or intimidated. How essential privacy is for democracy can also be seen with a counter example: totalitarian states purposely give their citizens as little privacy as possible in order to prevent them from developing an individual, autonomous personality. A uniform society without privacy is the goal of a dictatorship. What does that mean for data protection law? It nor only protects citizens' personal data and thus their human dignity and informational sef-determination. Data protection is also absolutely essential for a living democracy. Without data protection, the citizens' autonomy is threatened, and without this, a democracy cannot function. In short: data protection is a condition sine qua non for democracy.[12]

12 Tradução livre: "Mentes livres são a base das sociedades livres. Não é de admirar que o voto secreto seja um importante instrumento de eleições democráticas e o símbolo da democracia. Isso garante que as pessoas possam votar livre e autonomamente, sem serem observadas, coagidas ou intimidadas. Como a privacidade é essencial para a democracia também pode ser visto com um contraexemplo: os estados totalitários propositalmente dão a seus cidadãos o mínimo de privacidade possível para impedi-los de desenvolver uma personalidade individual e

Por fim, é pertinente salientar que os impactos do tratamento de dados pelo Poder Público vão além das particularidades legais, em comparação às normas estabelecidas ao setor privado, atingindo a esfera social sobremaneira, tendo em vista o crescente monitoramento das vidas dos indivíduos, potencializando eventual utilização das informações pessoais para fins indesejados e nocivos para os cidadãos e, em última análise, para as instituições democráticas.

CONSIDERAÇÕES FINAIS

Atribui-se grande valor aos dados pessoais na sociedade contemporânea, uma vez que são ferramentas essenciais para o progresso das tecnologias e do desenvolvimento dos Estados ao redor do globo, ao passo que ocorre, incessantemente, a virtualização da pessoa humana, em vista dos rastros virtuais deixados *online*. Consequentemente, impôs-se o aprimoramento das normas jurídicas para abarcar as demandas oriundas do meio digital e do protagonismo do fluxo informacional, de modo que o Brasil se enriqueceu com a promulgação da Lei Geral de Proteção de Dados.

As discussões acerca do tema continuam sendo pertinentes e relevantes, sendo que a pesquisa se propôs a analisar alguns dos principais pontos conflitantes da atualidade, quais sejam, o reconhecimento de um novo direito fundamental, diante da crescente necessidade de proteção eficaz aos dados pessoais, e o tratamento por parte do Poder Público. Constata-se que a proteção de dados pessoais deve ostentar natureza de direito fundamental, independente da privacidade, merecendo ser incluída entre as garantias constitucionais, inclusive, havendo o Projeto de Emenda à Constituição nº 17 visando tal fim, embora o posicionamento ainda não seja unânime.

Isso porque, a tutela aos dados pessoais abarca tanto aqueles da esfera pública, quanto os da esfera privada da vida do titular, tratando-se de proteção mais ampla, em vista da relevância de todo e qualquer tipo de dados na sociedade da informação. Vale ressaltar que, a LGPD é uma legislação específica, repleta de princípios e faculdades jurídicas próprias, fundamentando-se na autodeterminação informativa.

A partir da análise dos impactos das normas da LGPD, aplicáveis ao tratamento de dados pelo Poder Público, depreende-se que o uso de informações pessoais pode causar danos graves aos cidadãos e à sociedade, dependendo da atuação autônoma e eficaz da autoridade fiscalizadora.

Particularidades foram determinadas pela LGPD, visando facilitar a coleta de dados pessoais pelo Poder Público, por meio de maior abrangência de normas que dispensam o consentimento, porque, geralmente, o tratamento deve se dar para atender o interesse público.

Balanceando tal desequilíbrio, impõe-se a observância estrita do princípio da transparência,

autônoma. Uma sociedade uniforme sem privacidade é o objetivo de uma ditadura. O que isso significa para a lei de proteção de dados? Não protege apenas os dados pessoais dos cidadãos e, portanto, a sua dignidade humana e autodeterminação informativa. A proteção de dados também é absolutamente essencial para uma democracia viva. Sem proteção de dados, a autonomia dos cidadãos está ameaçada e, sem ela, a democracia não pode funcionar. Resumindo: a proteção de dados é uma condição sine qua non para a democracia." (BOEHME- NEßLER, 2016, p. 228).

criando o dever, ao Estado, de informar a motivação específica e a forma de operacionalização dos dados, ao titular. No entanto, o íntegro cumprimento das determinações legais depende da fiscalização, do poder investigativo e sancionatório do órgão de controle, a ANPD, sendo questionável sua independência, ante sua estruturação vinculada com a administração pública direta, fato que pode prejudicar a autonomia funcional e a atuação dos membros livremente nomeados pela Presidência da República.

Observa-se, além das medidas relacionadas à contenção da doença, movimentos do Governo Federal, como a criação do Cadastro Base do Cidadão e do Cadastro Nacional de Informações Sociais, em descompasso com as diretrizes da LGPD, que indicam pretensões de controle sobre os dados pessoais, postura adotada por governos autoritários, e que importam em violação às garantias constitucionais por discriminações decorrentes de técnicas de categorização dos indivíduos, maculando a autonomia e o desenvolvimento do ser político, pelo que vislumbra-se o descrédito e desconfiança nas instituições democráticas.

Em cotejo com o cenário de pandemia gerado pela Covid-19, constata-se que contextos emergenciais podem justificar a tomada de medidas abusivas e obscuras, acentuando ainda mais a vigilância constante e indesejada sobre os cidadãos.

Por fim, observa-se que a proteção de dados pessoais não deve sair dos holofotes dos debates jurídicos, uma vez que traz consigo definições e diretrizes que, necessariamente, precisam ser incorporadas pela sociedade, em prol do desenvolvimento e da segurança dos indivíduos e de seus dados.

REFERÊNCIAS

ABRUSIO, Juliana. Big data, internet das coisas e as cidades inteligentes. *In*: PIRES, Lilian Regina Gabriel Moreira (org.). Cidades inteligentes, humanas e sustentáveis: *In:* ENCONTRO INTERNACIONAL DE DIREITO ADMINISTRATIVO CONTEMPORÂNEO E OS DESAFIOS DA SUSTENTABILIDADE, 2., 2020, Belo Horizonte. **Anais** [...]. Belo Horizonte: Arraes Editores, 2020.

BARROS, Raphael Marques. "Quis custodiet ipsos custodies?": a naturalização da vigilância em massa em tempos de emergência. *In*: BIONI, Bruno Ricardo *et al.* (org.). **Os dados e o vírus**: pandemia, proteção de dados e democracia. São Paulo: Reticências Creative Design Studio, 2020.

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

BIONI, Bruno Ricardo. Xeque-mate: o tripé de proteção de dados pessoais no xadrez das iniciativas legislativas no Brasil. *In*: MACHADO, Jorge A. S.; ORTELLADO, Pablo; RIBEIRO, Márcio Moretto (org.). **Xeque-mate**: o tripé de proteção de dados pessoais no xadrez das iniciativas legislativas no Brasil. São Paulo: GPoPAI/USP, 2015.

BOEHME-NEßLER, Volker. Privacy: a matter of democracy. Why democracy needs privacy and data protection. **International Data Privacy Law**, Oxford, v. 6, n. 3, p. 222-229, 2016.

BRASIL. **Lei n. 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 [...]. Brasília, DF: Presidência da República, 2011. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 16 ago. 2020.

BRASIL. **Lei n. 13.709, de 14 agosto de 2018**. Lei geral de proteção de dados pessoais (LGPD). Brasília, DF: Presidência da República, 2018a. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 2 jun. 2020.

BRASIL. **Medida Provisória n° 869, de 2018**. 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, 2018b. Disponível em: https://www.congressonacional.leg.br/materias/medidas-provisorias/-/mpv/135062. Acesso em: 2 jun. 2020.

BRASIL. **Lei n. 13.979, de 6 fevereiro de 2020**. Dispõe sobre as medidas para enfrentamento da emergência de saúde pública de importância internacional decorrente do coronavírus responsável pelo surto de 2019. Diário Oficial da União: sessão 1, Brasília, DF: Presidência da República, p. 1, 2020a. Disponível em: https://www.in.gov.br/en/web/dou/-/lei-n-13.979-de-6-de-fevereiro-de-2020-242078735. Acesso em: 8 out. 2020.

BRASIL. **Medida provisória n. 954, de 17 abril de 2020**. Dispõe sobre o compartilhamento de dados por empresas de telecomunicações prestadoras de Serviço Telefônico Fixo Comutado e de Serviço Móvel Pessoal com a Fundação Instituto Brasileiro de Geografia e Estatística, para fins de suporte à produção estatística oficial durante a situação de emergência de saúde pública de importância internacional decorrente do coronavírus (covid-19), de que trata a Lei nº 13.979, de 6 de fevereiro de 2020. Brasília, DF: Presidência da República, 2020b. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/mpv/mpv954.htm. Acesso em: 10 ago. 2020.

BRASIL. Supremo Tribunal Federal. **ADI 6387**. Medida cautelar em ação direta de inconstitucionalidade. referendo. medida provisória nº 954/2020. Emergência de saúde pública de importância internacional decorrente do novo coronavírus (COVID-19). Relator Min. Rosa Weber, 28 de abril de 2020. Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=754357629. Acesso em: 10 ago. 2020.

CALABRICH, Bruno Freire de Carvalho. Discriminação algorítmica e transparência na lei geral de proteção de dados pessoais. **Revista de Direito e as Novas Tecnologias**, São Paulo, v. 8, jul./set. 2020. Disponível em: https://dspace.almg.gov.br/bitstream/11037/38411/1/Bruno%20Freire%20de%20Carvalho% 20Calabrich.pdf. Acesso em: 8 ago. 2020. DOI: https://doi.org/10.1093/idpl/ipw007

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico**, Joaçaba, v. 12, dez. 2011. Disponível em: https://portalperiodicos.unoesc.edu.br/espacojuridico/article/view/1315. Acesso em: 2 jun. 2020. Não citado

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**: fundamentos da lei geral de proteção de dados. 2. ed. São Paulo: Thomson Reuters Brasil, 2020.

GARCIA, Marco Aurélio Fernandes. Saúde e proteção de dados: fundamentos da vigilância

epidemiológica social. *In*: BIONI, Bruno Ricardo *et al*. (org.). **Os dados e o vírus**: pandemia, proteção de dados e democracia. São Paulo: Reticências Creative Design Studio, 2020.

GONÇALVES, Tânia Carolina Nunes Machado. **Gestão de dados pessoais e sensíveis pela Administração Pública Federal**: desafios, modelos e principais impactos com a nova lei. 2019. 147 f. Dissertação (Mestrado em Direito) - Centro Universitário de Brasília, Brasília, 2019.

GUARDIA, Andrés Felipe Thiago Selingardi. De surveillance a dataveillance: enfoque a partir da noção jurídica de tratamento de dados. **Revista dos Tribunais Online**, São Paulo, v. 109, n. 1012, p. 494, fev. 2020. Disponível em: https://www.mprj.mp.br/documents/20184/0/revistadostribunaisn.1012.pdf. Acesso em: 2 jun. 2020.

KITAYAMA, Marina Sayuri. Dados pessoais e coronavírus, do abuso à legitimidade. *In*: BIONI, Bruno Ricardo *et al.* (org.). **Os dados e o vírus**: pandemia, proteção de dados e democracia. São Paulo: Reticências Creative Design Studio, 2020.

LEONARDI, Marcel. **Tutela e privacidade na internet**. São Paulo: Saraiva, 2011.

MARTINS, Pedro Bastos Lobo; HOSNI, David Salim Santos. O livre desenvolvimento da identidade pessoal em meio digital: para além da proteção da privacidade? *In*: POLIDO, Fabrício; ANJOS, Lucas; BRANDÃO, Luíza (org.). **Políticas, internet e sociedade**. Belo Horizonte: Instituto de Referência em Internet e Sociedade, 2019. p. 46-54.

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

MENDES, Laura Schertel; DONEDA, Danilo. Comentário à nova lei de proteção de dados (lei 13.709/2018): o novo paradigma da proteção de dados no Brasil. **Revista de Direito do Consumidor**, Brasília, v. 120, p. 555-587, nov./dez. 2018.

MENDES, Laura Schertel; DONEDA, Danilo. Marco jurídico para a cidadania digital: uma análise do projeto de lei 5.276/2016. **Revista de Direito Civil Contemporâneo**, São Paulo, v. 9, 2016. Disponível em: http://ojs.direitocivilcontemporaneo.com/index.php/rdcc/article/view/171. Acesso em: 5 out. 2020.

MENDES, Laura Schertel; FONSECA, Gabriel Campos Soares da. STF reconhece direito fundamental à proteção de dados. **Revista de Direito do Consumidor**, São Paulo, n.130, jul./ago. 2020. Disponível em: https://dspace.almg.gov.br/handle/11037/38077. Acesso em: 9 ago. 2020.

PINHEIRO, Patrícia Peck Garrido. Nova lei brasileira de proteção de dados pessoais (LGPD) e o impacto nas instituições públicas e privadas. **Revista dos Tribunais**, São Paulo, n.1000, fev. 2019. Disponível em: https://dspace.almg.gov.br/handle/11037/32749. Acesso em: 7 ago. 2020.

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

RANIERI, Nina Beatriz Stocco. **Teoria do Estado**: do estado de direito ao estado democrático de direito. Barueri: Manole, 2013.

SCOPEL, Adriano Sayão. Breves considerações sobre tratamento de dados pelo poder público e

meios de defesa dos dados pessoais por particulares. **Revista de Direito e as Novas Tecnologias,** São Paulo, n. 7, abr./jun. 2020. Disponível em: https://dspace.almg.gov.br/handle/11037/37757. Acesso em: 16 ago. 2020.

SILVA, Daniela Juliano. Govtech à brasileira: o plano nacional de internet das coisas e o cadastro base do cidadão. *In*: LEAL, Fernando; MENDONÇA, José Vicente Santos de (org.). **Transformações do direito administrativo**: liberdades econômicas e regulação. Rio de Janeiro: Fgv Direito Rio, 2019.

SIMÃO, Bárbara; OMS, Juliana; TORRES, Livia. **Autoridades de proteção de dados na América Latina**: um estudo dos modelos institucionais da Argentina, Colômbia e Uruguai. São Paulo: IDEC, 2019.

Recebido em: 29/05/2021
Aceito em: 12/11/1022