PARECER

Exma. Sra. Presidente da Comissão de Proteção de Dados e Privacidade
da Ordem dos Advogados do Brasil do Estado do Rio de Janeiro,

Dra. Estela Aranha

Referência: Elaboração de parecer sobre a legalidade dos Decretos nº 10.046/2019 e nº 10.047/2019 em face das normas que disciplinam os direitos fundamentais à proteção de dados e à privacidade no ordenamento jurídico brasileiro.

1- A Economia dos Dados e a Autodeterminação Informativa. 1.1- A relação assimétrica dos titulares dos dados pessoais com os detentores das tecnologias: Como garantir a efetiva proteção dos titulares de dados pessoais? 2- O reconhecimento da proteção de dados pessoais como direito fundamental no ordenamento jurídico brasileiro. 3- A edição dos Decretos nº 10.046/2019 e nº 10.047/2019: riscos para a privacidade e para a proteção de dados pessoais. 4- Conflitos dos Decretos nº 10.046/2019 e nº 10.047/2019 em face das normas constitucionais e legais – Pressupostos metodológicos. 5- Conceitos jurídicos e regras específicas do Decreto nº 10.046/2019 conflitantes com a Constituição Federal e com a Lei Geral de Proteção de Dados Pessoais. 5.1- Natureza Jurídica do Decreto nº 10.046/2019 e o controle de constitucionalidade: trata-se de um decreto regulamentar ou estamos diante de um legítimo decreto autônomo? 5.2- Revogação do Decreto nº 8.789/2016 e as incompatibilidades do Decreto nº 10.046/2019 com os fundamentos e princípios da Lei Geral de Proteção de Dados Pessoais. 5.3- Criação de novos conceitos de dados pessoais alheios à LGPD: Ampliação da coleta de dados pessoais sensíveis e criação de um sistema de vigilância massivo? 5.4- Riscos imediatos relativos à Segurança da Informação: a LGPD será relegada a um caráter meramente decorativo? 5.5- Superposição de Órgãos, Problemas de Governança, de Fiscalização e de *Enforcement*. 5.6- Da necessidade de harmonização das normas atinentes à proteção de dados em consonância com as regras de transferência internacional de dados. 5.7- A irresponsabilidade administrativa, sendo fonte de insegurança jurídica e gerando impactos econômicos negativos. 6- Precedentes do Supremo Tribunal Federal: Restrições ao Compartilhamento de Dados entre Órgãos da Administração

Pública e Vedação ao "Constitucionalismo Abusivo". 6.1- Decisões que restringem o compartilhamento de dados entre órgãos da Administração Pública (áreas administrativa e cível). 6.2- Os riscos do "constitucionalismo abusivo", que promove retrocesso democrático e violação a direitos fundamentais. 7- Conclusão.

1- A ECONOMIA DOS DADOS E A AUTODETERMINAÇÃO INFORMATIVA

As transformações digitais, o crescimento da nova economia dos dados e a ascensão da chamada 4ª Revolução Industrial vêm promovendo imensos desafios para a garantia dos direitos fundamentais dos indivíduos, de forma que estes direitos sejam preservados em harmonia com o desenvolvimento econômico e tecnológico.

O aumento do poder computacional, a expansão da inteligência artificial, a progressiva capacidade técnica de coleta e tratamento dos dados – tanto pelo setor privado, quanto pelo Estado – estão conduzindo a um fluxo exponencial de informações pessoais que são utilizadas para diversas finalidades – algumas benéficas para a sociedade e outras perigosas ou obscuras.

Entidades internacionais como a OCDE – Organização para a Cooperação e Desenvolvimento Econômico – e a ONU têm demonstrado grande preocupação com a necessidade de implementação de legislações nacionais que promovam adequadamente a proteção dos direitos dos consumidores e dos cidadãos em relação aos seus dados pessoais, compatibilizando-se estes direitos com a inovação digital e o progresso econômico e tecnológico, a fim de que se assegure a transferência (nacional e internacional) dos dados com segurança, boas práticas e alto nível de governança.

Com a edição da Lei nº 13.709, em 14/08/2018, a chamada LGPD[1] – Lei Geral de Proteção de Dados Pessoais –, o Brasil passou a integrar o grupo de mais de 130 países que possuem a sua própria lei de proteção dos dados pessoais. Deve-se destacar que o texto original da LGPD teve alguns dispositivos modificados pela Lei nº 13.853/2019, especialmente no tocante à constituição e ao funcionamento da Autoridade Nacional de Proteção de Dados (ANPD) e do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade.

A *LGPD foi inspirada na GDPR*[2]*, regulação de proteção de dados da União Europeia*, como aludido por seu relator, Deputado Federal Orlando Silva, no curso do processo legislativo que culminou com a aprovação da lei.[3] O regulamento da União Europeia entrou em vigor em maio de 2018, após o prazo de 2 anos de vacância legal, enquanto

[1] Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 30 de outubro de 2019.

[2] A GDPR – *General Data Protection Regulation* – é a regulação de proteção de dados do direito comunitário europeu (da União Europeia) que disciplina a proteção dos dados pessoais e estabelece normas para que as empresas e os Estados atuem para atingir as finalidades da lei. A GDPR entrou em vigor em maio de 2018 e substituiu a Diretiva de Proteção de Dados Pessoais 95/46/CE.

[3] Disponível em: <https://porta23.blogosfera.uol.com.br/2018/05/29/camara-aprova-pl-de-protecao-de-dados-pessoais-e-envia-para-o-senado/>. Acesso em: 25 de novembro de 2019.

a LGPD ainda se encontra em período de *vacatio legis*, tendo sido disciplinado que entrará em vigor em agosto de 2020.[4]

Um dos aspectos cruciais relativos à legislação de proteção de dados encontra as suas raízes nas Diretrizes da OCDE para a Proteção da Privacidade e dos Fluxos Transfronteiriços de Dados Pessoais[5], de 1980, que representam um consenso internacional sobre princípios e regras relativos à coleta e ao gerenciamento da informação pessoal e que se apoiam em três princípios comuns aos países membros da OCDE: democracia pluralista, respeito aos direitos humanos e economias de mercado aberto.

Com bastante atraso e após debates que duraram quase uma década, o Brasil finalmente aprovou a LGPD para acompanhar as mudanças vertiginosas das tecnologias e infraestruturas de informação e de comunicação e para garantir o nível de proteção adequado de privacidade e de fluxos de dados pessoais, tanto nacional quanto internacionalmente – o que gerará benefícios e avanços econômicos e sociais. Como bem esclareceu o Deputado Federal Orlando Silva, "é importante que o Brasil avance na regulação, inclusive para ter uma legislação compatível com a da União Europeia, que considera que as parcerias econômicas com a OCDE acontecerão em função da existência de normas compatíveis nesses países".[6]

A LGPD e a GDPR assentam-se na *autodeterminação informacional ou informativa*, que visa a conceder aos titulares dos dados pessoais um real poder sobre as suas próprias informações e um efetivo controle sobre os seus dados. A autodeterminação informativa, ao lado do respeito à privacidade e de outros paradigmas normativos, está prevista como um dos fundamentos da LGPD, no inciso II do seu art. 2º.

A *autodeterminação informativa* teve seu marco jurisprudencial determinado a partir da famosa decisão do Tribunal Constitucional da então Alemanha Ocidental[7], em 1983, na qual foi declarada inconstitucional uma lei que criava um censo estatal que determinava a coleta de dados pessoais dos cidadãos para a otimização de políticas públicas. Esta decisão pioneira apontou para a necessidade de reconceituação da divisão de poderes na nascente sociedade de informação da época.

A referida lei do censo alemão previa que cada cidadão deveria responder a 160 perguntas, a serem posteriormente submetidas a tratamento informatizado. Como elucida Danilo Doneda, alguns pontos da lei geraram controvérsia e "fomentaram um sentimento generalizado de insegurança, aliado à impressão de que o governo poderia

[4] Foi apresentado, em 30/10/2019, o PL 5762/2019, de autoria do Deputado Federal Carlos Bezerra (MDB-MT), objetivando postergar a entrada em vigor da LGPD para 15/08/2022. Foi apresentada, como uma das justificativas para o adiamento da *vacatio legis* da LGPD, a "morosidade" do Poder Executivo na instalação da Autoridade Nacional de Proteção de Dados (ANPD).

[5] Disponível em: <http://www.oecd.org/sti/ieconomy/15590254.pdf>. Acesso em: 25 de novembro de 2019.

[6] Disponível em: <https://porta23.blogosfera.uol.com.br/2018/05/29/camara-aprova-pl-de-protecao-de-dados-pessoais-e-envia-para-o-senado/>. Acesso em: 25 de novembro de 2019.

[7] BVerfGE 65, 1 – Volkszählung

se valer dos dados obtidos – que a princípio serviriam a finalidades estatísticas – para realizar um controle capilar das atividades e da condição pessoal dos cidadãos".[8]

Entidades da sociedade civil organizada e alguns comissários de proteção de dados pessoais iniciaram um debate e chamaram a atenção para os problemas que o censo poderia acarretar aos cidadãos. "Este protesto deu origem ao processo que provocou a sentença da Corte Constitucional, suspendendo provisoriamente o censo e declarando que a lei que o instituía era inconstitucional em relação aos artigos 1.1 e 2.1 da Lei Fundamental, exatamente a base sobre a qual se estrutura o direito geral da personalidade – *allgemeines Persönlichkeitsrecht* ".[9]

É importante destacar que, entre os motivos e argumentos que levaram a Corte Constitucional Alemã a reconhecer essa inconstitucionalidade, muitas questões se assemelham ao que discutiremos neste parecer acerca dos Decretos nº 10.046/2019 e nº 10.047/2019:

a) diversidade de finalidades, que impediria que o cidadão conhecesse o uso efetivo que seria feito de suas informações;

b) desmistificação da noção que o tratamento de certos tipos de dados pessoais seria irrelevante para a privacidade;

c) o estágio de desenvolvimento da tecnologia informática utilizada no processamento das informações levantadas com o censo era um fator determinante, visto que a elaboração de perfis formados sobre dados dos indivíduos teria potencial ilimitado e prováveis resultados danosos aos direitos individuais.

Destaca-se, por conseguinte, que nos contornos delineados pelo Tribunal Constitucional Alemão a autodeterminação informativa teria uma dimensão democrática, a fim de propiciar categórica transparência em relação aos motivos e às finalidades do tratamento dos dados pessoais. Uma segunda dimensão da autodeterminação informativa seria ligada ao controle efetivo do titular dos dados em relação à exatidão das informações e à real utilização dos seus dados pessoais.

Atualmente, é importante consignar que o fenômeno da convergência em torno de leis gerais, na Europa e na América Latina, fundadas em direitos básicos concedidos aos titulares de dados e no conjunto de obrigações aos controladores e processadores de dados, vem trazendo novas reflexões acerca da crescente (hiper) vulnerabilidade dos titulares dos dados pessoais e do ressignificado do consentimento como o pilar normativo das leis gerais de proteção de dados, como propõe Bruno Bioni [10].

---

[8] DONEDA, Danilo. *Da Privacidade à Proteção de Dados Pessoais*. Rio de Janeiro: Renovar, 2006. p. 193.

[9] DONEDA, Danilo. *Da Privacidade à Proteção de Dados Pessoais*. Rio de Janeiro: Renovar, 2006. p. 194.

[10] BIONI, Bruno Ricardo. *Proteção de Dados Pessoais* – a função e os limites do consentimento. Rio de Janeiro: Forense, 2019, p. 274: "Ao longo desse percurso, verificou-se que o *consentimento* do titular dos dados *continua a exercer um papel normativo de protagonismo, mas sob um novo roteiro que inclui a atuação de atores coadjuvantes importantes: i)* novas formas para operacionalizá-lo, levando-se em conta a arquitetura (de vulnerabilidade) da rede; *ii)* o relato normativo complementar da privacidade contextual que o limita e o readapta diante de um solo epistemológico que esfacela a técnica tradicional da autodeterminação baseada de declaração de vontade do titular dos dados; e *iii)* o cidadão também exerce domínio sobre seus

1.1- A RELAÇÃO ASSIMÉTRICA DOS TITULARES DOS DADOS PESSOAIS COM OS DETENTORES DAS TECNOLOGIAS: COMO GARANTIR A EFETIVA PROTEÇÃO DOS TITULARES DE DADOS PESSOAIS?

Diante da crescente relação assimétrica dos titulares de dados pessoais com os detentores das tecnologias – empresas (tanto Big Techs *como* startups *que coletam enorme quantidade de dados pessoais) e Estados –, torna-se urgente não apenas a concretude do paradigma da autodeterminação informativa, mas a adoção de novas formas de proteção dos direitos dos titulares de dados*. Sem o avanço mais amplo desses novos modelos de proteção, assistiremos à materialização dos riscos sinalizados por vozes autorizadas, como Yuval Harari, que apontam para a possibilidade de ascensão de verdadeiras "ditaduras digitais baseadas em tecnologias digitais de vigilância" nos próximos dez ou vinte anos: "Podemos prever (...) a ascensão dessas ditaduras digitais, ditaduras baseadas em tecnologias digitais de vigilância que seguem tudo o tempo todo. Podemos prever que isso acontecerá não só nos países mais desenvolvidos, mas até em alguns países mais atrasados do mundo, na África e no Oriente Médio".[11]

As advertências do historiador e filósofo israelense devem ser objeto de profunda reflexão, na medida em que nos alertam para as formas insidiosas de manipulação dos indivíduos pelos poderosos detentores das tecnologias – Estados ou empresas – e nos colocam diante de instigantes questionamentos jurídicos, filosóficos e éticos: Quem é o dono dos dados? Os dados mais íntimos e sensíveis dos seres humanos – do DNA, de saúde, das opiniões e pensamentos – pertencem realmente aos seus titulares?[12]

> À medida que, através de sensores biométricos, cada vez mais dados fluírem de seu corpo e de seu cérebro para máquinas inteligentes, será fácil para corporações e agências do governo conhecer você, manipular você e tomar decisões por você. Mais importante ainda, eles serão capazes de decifrar os mecanismos profundos de todos os corpos e cérebros, e com isso adquirir o poder de fazer a engenharia da vida. Se quisermos evitar que uma pequena elite monopolize esses poderes, que parecem divinos, e se quisermos impedir que a humanidade se fragmente em castas biológicas, a questão-chave é: quem é dono dos dados? Os dados de meu DNA, meu cérebro e minha vida pertencem a mim, ao governo, a uma corporação ou ao coletivo humano?[13]

---

dados, se estes forem tratados de forma previsível de acordo com suas legítimas expectativas. Portanto, o conteúdo jurídico-normativo de autodeterminação informacional vai além do consentimento."

[11] Disponível em: <https://www.uol.com.br/tilt/noticias/redacao/2019/11/11/escritor-yuval-harari-roda-viva-entrevista.htm>. Acesso em: 25 de novembro de 2019.

[12] Lamentavelmente, ainda não temos a cultura da privacidade e da proteção de dados consolidada no Brasil. Muitas pessoas não têm consciência do valor dos seus bens mais valiosos – os seus dados pessoais. Pior do que isso, não têm noção dos riscos envolvidos nessa entrega deliberada e inconsciente dos seus dados, muito menos dos prejuízos que incidentes e vazamentos de dados podem ocasionar aos seus titulares.

[13] HARARI, Yuval Noah. *21 lições para o século 21*. São Paulo: Companhia das Letras, 2018. p. 109.

Em dezembro de 2019, o Ministério da Ciência, Tecnologia, Inovações e Comunicações (MCTIC) lançou uma consulta pública[14], com prazo até 31 de janeiro de 2020, para a elaboração de uma Estratégia Nacional de Inteligência Artificial. Dividida em três eixos transversais e seis verticais, o documento traz uma série de perguntas, as quais, diante da sua complexidade e da exiguidade do período da consulta, correm o risco de restringir a participação a poucos especialistas e acadêmicos, não abrangendo toda a sociedade. A importância da consulta pública é enorme, visto que a IA trará profundas mudanças na economia, no governo e na sociedade e as discussões sobre os seus impactos, positivos e negativos, vêm ocorrendo em outros países e organismos internacionais, como a OCDE.

Uma das tecnologias mais preocupantes para os especialistas em segurança da informação e proteção de dados é *o reconhecimento facial*, considerado por Luke Stark, pesquisador da *Microsoft Research*, o *"Plutônio da Inteligência Artificial"*.[15] Entidades e vozes abalizadas em todo o mundo têm apontado os mais diversos riscos dessa tecnologia. Várias cidades do mundo, como São Francisco, estão proibindo o uso de reconhecimento facial, tanto na esfera pública quanto nos ambientes privados, justamente em razão da falta de transparência e de mecanismos garantidores de que essa tecnologia será usada para finalidades exclusivas de segurança, sem riscos de violações a direitos fundamentais, e com alto nível de transparência e *accountability*.

No Brasil, cidades como o Rio de Janeiro e Salvador vêm ampliando o uso de câmeras de monitoramento com sistemas de reconhecimento facial com o principal objetivo de identificar pessoas com mandados de prisão em aberto, de forma que a Polícia Militar seja imediatamente alertada e promova a prisão do indivíduo reconhecido. Erros no sistema de reconhecimento facial já foram divulgados por órgãos de imprensa, contudo, desconhecemos a publicação de estatísticas em relação a esses erros, bem como, não identificamos a adoção de procedimentos oficiais de auditagem desses sistemas.[16]

Organizações da sociedade civil têm solicitado a diferentes órgãos de segurança pública o acesso à informação com base na LAI – Lei de Acesso à Informação – para melhor compreender a gestão dos sistemas de reconhecimento facial. Joana Varon, Diretora Executiva da *Coding Rights*, vem defendendo publicamente que diversos casos no Brasil – e em outros países que adotaram recentemente o uso de reconhecimento facial para fins de segurança pública – *"mostram que há tanto a propensão a abuso policial, como de abusos por parte do setor privado, tendo em vista que sua implementação*

[14] Disponível em: <http://www.mctic.gov.br/mctic/opencms/salaImprensa/noticias/arquivos/2019/12/MCTIC_lanca_consulta_publica_para_a_Estrategia_Brasileira_de_Inteligencia_Artificial.html>. Acesso em: 20/12/2019.

[15] *V.* Artigo de Luke Stark, Pesquisador na *Microsoft Reserch* Montreal. Disponível em: <https://static1.squarespace.com/static/59a34512c534a5fe6721d2b1/t/5cb0bf02eef1a16e422015f8/1555087116086/Facial+Recognition+is+Plutonium+-+Stark.pdf>. Acesso em 01 de dezembro de 2019.

[16] Disponível em: <https://g1.globo.com/rj/rio-de-janeiro/noticia/2019/07/11/sistema-de-reconhecimento-facial-da-pm-do-rj-falha-e-mulher-e-detida-por-engano.ghtml>. Acesso em 01 de dezembro de 2019.

envolve compartilhamento de dados sensíveis com as empresas privadas que implementam esses sistemas".[17]

Autoridades como a *European Union Agency for Fundamental Rights* estão conduzindo estudos para formular proposições destinadas à regulação ética e jurídica do reconhecimento facial[18] e de outras tecnologias de inteligência artificial – IA. No tocante ao reconhecimento facial, recente notícia divulgada pelo site *Politico Europe* informa que foi elaborada, por Margrethe Vestager[19], uma minuta sugerindo proibir o uso do reconhecimento facial nos espaços públicos nos países da União Europeia, pelo período de três a cinco anos, até que existam salvaguardas para mitigar os riscos dessa tecnologia.[20]

No amplo contexto da IA, destacam-se as *Diretrizes da União Europeia sobre Inteligência Artificial e Proteção de Dados,*[21] *no âmbito do Comitê Consultivo da Convenção 108 do Conselho da Europa. Estas diretrizes preconizam que o desenvolvimento e o uso da IA devem respeitar os direitos humanos e as liberdades fundamentais, em especial os direitos à privacidade e à proteção dos dados pessoais.*[22]

A CNIL (Autoridade Supervisora Francesa) publicou recentemente um guia sobre o uso do reconhecimento facial, dirigido especialmente às autoridades públicas francesas. O material apresenta questões conceituais, bem como os riscos, as vantagens e as regras de uso da nova tecnologia.[23]

Deve-se destacar que as decisões automatizadas têm levantado discussões intensas sobre como o desenvolvimento exponencial da Inteligência Artificial tem conduzido à opacidade, vieses e injustiças, como denuncia o trabalho da matemática e cientista de dados Cathy O´Neil. Ela levantou situações recorrentes em que o uso de algoritmos se consolida em um instrumento para *aumentar as desigualdades socioeconômicas inerentes aos sistemas capitalistas, reforçando a discriminação social derivada da raça e da classe social e transformando-se em uma ameaça à própria democracia.*[24]

---

[17] Disponível em: <https://medium.com/codingrights/bem-na-sua-cara-a-ilusão-do-reconhecimento-facial-para-segurança-pública-47c708b34820>. Acesso em 30 de outubro de 2019.

[18] Disponível em: <https://fra.europa.eu/en/publication/2019/facial-recognition>. Acesso em: 01 de dezembro de 2019.

[19] Margrethe Vestager é Vice-Presidente Executiva da Europe Fit for the Digital Age. Disponível em: <https://ec.europa.eu/commission/commissioners/2019-2024/vestager_en>. Acesso em: 17 de janeiro de 2020.

[20] Disponível em: <https://www.politico.eu/pro/eu-considers-temporary-ban-on-facial-recognition-in-public-spaces/>. Acesso em: 17 de janeiro de 2020.

[21] Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention 108). Disponível em: <https://rm.coe.int/guidelines-on-artificial-intelligence-and-data-protection/168091f9d8>. Acesso em: 20 de novembro de 2019.

[22] Neste sentido, *v.* FERREIRA, Lucia Maria Teixeira. Novas Tecnologias, Cidadania e o Cuidado: Premissas para a Regulação Jurídica da Inteligência Artificial. *In: PEREIRA*, Tania da Silva; OLIVEIRA, Guilherme de; COLTRO, Antônio Carlos Mathias (Coord.). *Cuidado e Cidadania*: Desafios e Possibilidades. Rio de Janeiro: GZ, 2019, p. 341-365.

[23] Disponível em: <https://www.cnil.fr/sites/default/files/atoms/files/reconnaissance_faciale.pdf>. Acesso em: 01 de dezembro de 2019.

[24] O'NEIL, Cathy. *Weapons of Mass Destruction:* How Big Data Increases Inequality and Threatens Democracy. Denver: Crown, 2016.

Na realidade, fora dos círculos altamente restritos e especializados, pouco se conhece dos sistemas de *machine learning* e *deep learning*. Como salienta Ana Frazão, "é difícil julgar ética e juridicamente algo que pouco se conhece. Nesse sentido, os algoritmos têm se mostrado verdadeiras caixas pretas, pois, salvo seus desenvolvedores, normalmente ninguém sabe ao certo como funciona o seu poder de ação e predição: nem os usuários nem aqueles que sofrerão as consequências da referida decisão".[25]

É fundamental que se promova a conscientização na sociedade, nas empresas e nos órgãos públicos sobre a real necessidade de coleta e armazenamento de dados pessoais, além da dimensão da extensão dessa coleta, haja vista que, quanto maiores forem a quantidade e a diversidade dos dados coletados e a complexidade do processamento, maiores serão os riscos e as dificuldades de se entender a *ratio* das decisões automatizadas.

Novos modelos de regulação ética e jurídica estão sendo propostos e definidos em outros países. A Cidade de Nova York teve uma interessante iniciativa: criou o cargo de *"Chief Algorithms Officer Position"*, que funcionará fora do escritório do Prefeito Bill de Blasio e conduzirá o desenvolvimento de diretrizes e melhores práticas em torno do uso de ferramentas baseadas em algoritmos nas agências da cidade.[26]

Iniciativas como as do *Information Commissioner´s Office* (ICO), a autoridade de proteção de dados britânica, também devem ser incentivadas, como a criação de novas estruturas para auditoria de sistemas de IA baseadas em governança e responsabilidade, bem como, na identificação de riscos específicos da IA. Outra promissora iniciativa do ICO é a promoção de *sandbox* regulatório destinado a apoiar organizações que usam dados pessoais e que podem desenvolver produtos e serviços inovadores com benefício público demonstrável.[27]

2- O RECONHECIMENTO DA PROTEÇÃO DE DADOS PESSOAIS COMO DIREITO FUNDAMENTAL NO ORDENAMENTO JURÍDICO BRASILEIRO

No direito brasileiro, muito antes da edição da LGPD, as bases principiológicas do direito à proteção de dados pessoais já poderiam ser encontradas em diversos dispositivos constitucionais e na legislação infraconstitucional.

[25] Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/algoritmos-e-inteligencia-artificial-15052018>. Acesso em: 07 de novembro de 2019. Ana Frazão analisa as repercussões que a transferência de decisões para algoritmos apresenta no âmbito da responsabilidade civil e punitiva, ressaltando que "a delegação das decisões e escolhas para as máquinas não pode ser vista como uma alternativa isenta de responsabilidades no plano jurídico, dando ensejo ao processo que alguns já chamam de *mathwashing*. A questão a ser enfrentada aqui é saber em que medida podemos terceirizar nossas responsabilidades para máquinas e quais as repercussões jurídicas disso".

[26] Disponível em: <https://www.govtech.com/products/New-York-City-Creates-Chief-Algorithms-Officer-Position.html>. Acesso em: 01 de dezembro de 2019.

[27] Disponível em: <https://ico.org.uk/about-the-ico/our-information/our-strategies-and-plans/>. Acesso em: 30 de novembro de 2019.

Renomados juristas entendiam que *a privacidade era o* locus *constitucional da proteção de dados*, no sentido de que os dados pessoais se constituíam em elemento constituinte da identidade da pessoa e, desta forma, os dados deveriam ser protegidos como parte fundamental da personalidade humana.

Neste diapasão, o reconhecimento do direito à proteção de dados pessoais efetiva-se através de diversos dispositivos da Constituição da República que protegem a intimidade, a vida privada, a honra e a imagem: a partir da proteção da intimidade (art. 5º, X, da Constituição Federal), que abrange a proteção à própria imagem em face, inclusive, dos meios de comunicação de massa; do direito à informação (art. 5º, XIV); do direito ao sigilo das comunicações e dados (art. 5º, XII); da inviolabilidade do domicílio (art. 5º, XI); do direito a receber dos órgãos públicos informações de seu interesse ou de interesse coletivo ou geral, com exceção daquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado (art. 5º, XXXIII); ou da garantia individual ao conhecimento e correção de informações sobre si pelo *habeas data* (art. 5º, LXXII).

A própria legislação infraconstitucional – contida no Código de Defesa do Consumidor, na Lei do Cadastro Positivo, na Lei de Acesso à Informação e no Marco Civil da Internet – criava, como afirma Laura Schertel[28], uma *obrigação positiva para o Estado*, o qual deveria agir para garantir a efetiva tutela do direito à proteção de dados. Este entendimento doutrinário embasou a investigação e a propositura de diversas ações civis públicas para a defesa dos titulares de dados pessoais em situações de vazamentos de dados, em incidentes de segurança ou em uso indiscriminado de dados dos consumidores, que levaram a condenações e multas.[29]

Ao longo das últimas décadas, entretanto, foi-se construindo a configuração do *direito à proteção de dados* como *um novo direito fundamental, destacado e independente do direito à privacidade*[30], com a identificação de uma série de liberdades individuais, atreladas ao direito à proteção de dados pessoais, que não são abraçadas pelo direito à privacidade. E o "centro gravitacional da proteção dos dados pessoais é diferente do direito à privacidade – *i.e.*, a percepção de que a sua tutela jurídica opera fora da dicotomia do público e do privado". [31]

Por conseguinte, fez-se necessária uma *atualização constitucional para que se reconhecesse a proteção de dados pessoais como direito fundamental autônomo em relação ao direito à privacidade, entendimento este que embasou a formulação da Proposta de Emenda Constitucional nº 17/2019, a qual inclui na Constituição Federal, no rol dos direitos fundamentais do art. 5º, o inciso LXXIX ("o direito à proteção dos dados*

[28] MENDES, Laura Schertel. *Privacidade, Proteção de Dados e Defesa do Consumidor*: Linhas Gerais de um Novo Direito Fundamental. São Paulo: Saraiva, 2014.
[29] Drogaria Araújo, de Minas Gerais, é multada em 8 milhões por pedir CPF de clientes. Notícia disponível em: <https://www.em.com.br/app/noticia/economia/2018/12/06/internas_economia,1011120/drogaria-araujo-e-multada-em-quase-r-8-milhoes-por-pedir-cpf-de-clien.shtml>. Acesso em: 31 de outubro de 2019.
[30] Destacamos que está fora do escopo deste artigo a discussão sobre eventuais equívocos na construção dogmática do direito à proteção de dados como *mera* evolução do direito à privacidade. Para maior aprofundamento, recomendo a obra de Bruno Bioni citada na N.R. seguinte.
[31] BIONI, Bruno Ricardo. *Proteção de Dados Pessoais* – a função e os limites do consentimento. Rio de Janeiro: Forense, 2019, p. 99.

pessoais, inclusive nos meios digitais"), além de acrescentar ao art. 22 o inciso XXX (a proteção e tratamento de dados pessoais como matéria de competência legislativa privativa da União).[32]

O relator da PEC 17/2019, Deputado Federal Orlando Silva – que também foi o relator da LGPD –, inseriu um novo dispositivo normativo na PEC, o qual constitucionaliza a Agência Nacional de Proteção de Dados no formato de uma agência reguladora.[33] Trata-se do acréscimo do inciso XXVI ao art. 21 da Constituição Federal – que cuida das competências da União – com a seguinte redação:

> *Art. 21. Compete à União:*
>
> *(...)*
>
> *XXVI – organizar e fiscalizar a proteção e o tratamento de dados pessoais, nos termos da lei, que disporá sobre a criação de um órgão regulador e outros aspectos institucionais.*

Deve-se consignar que, no tocante às competências legislativas da União, o relatório endossa *a competência privativa da União para legislar sobre a matéria, prevendo a possibilidade da edição de leis que abordem a questão do tratamento e proteção de dados pessoais de forma indireta, no âmbito e competência legislativa de Estados e Municípios,* em consonância com a LGPD, como nos casos de assuntos de interesse local e serviços públicos de interesse local, incluído o transporte coletivo.

A Comissão Especial sobre Dados Pessoais aprovou, na íntegra, o substitutivo apresentado pelo Deputado Federal Orlando Silva na sessão ocorrida em 10/12/2019.[34] Em seguida, a PEC 17/2019 seguirá para o Plenário da Câmara dos Deputados para votação em dois turnos. Considerando-se a aprovação do substitutivo do relator, que incluiu um novo dispositivo à PEC (o inciso XXVI ao art. 21 da Constituição Federal), a PEC 17/2019 deverá retornar ao Senado Federal para nova votação.

3- A EDIÇÃO DOS DECRETOS Nº 10.046/2019 E Nº 10.047/2019: RISCOS PARA A PRIVACIDADE E PARA A PROTEÇÃO DE DADOS PESSOAIS

No atual panorama jurídico, causou dúvida e preocupação a edição de dois Decretos pelo Presidente da República, por levantarem sérios questionamentos em relação às normas que regulam a privacidade e a proteção de dados pessoais no Brasil:

---

[32] Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/135594> e <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2210757>. Acesso em: 31 de outubro de 2019.

[33] Disponível em: <https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=21E55F45F3DB465585226243BA4ADE60.proposicoesWeb2?codteor=1841176&filename=PRL+1+PEC01719+%3D%3E+PEC+17/2019>. Acesso em: 17 de dezembro de 2109.

[34] Disponível em: <https://www.camara.leg.br/noticias/624541-comissao-aprova-proposta-que-insere-protecao-de-dados-pessoais-na-constituicao/>. Acesso em: 17 de dezembro de 2019.

o Decreto nº 10.046 e o Decreto nº 10.047, ambos de 09 de outubro de 2019. Estas normas infralegais, especialmente a primeira, suscitaram diversas indagações sobre eventuais riscos e impactos danosos à privacidade e à proteção de dados pessoais de todos os brasileiros.

O Decreto nº 10.046/2019 "dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados"[35].

O Decreto nº 10.047/2019 "dispõe sobre a governança do Cadastro Nacional de Informações Sociais e institui o programa Observatório de Previdência e Informações, no âmbito do Cadastro Nacional de Informações Sociais"[36].

Até a edição dos referidos decretos, o modelo de compartilhamento de dados na administração federal era aquele definido pelo Decreto nº 8.789/2016, regulamentado pela Portaria nº 58/2016, da Secretaria de Tecnologia da Informação. O Decreto nº 8.789/2016 foi revogado pelo Decreto nº 10.046/2016, o qual, em conjunto com a outra deliberação do Chefe do Poder Executivo Federal (Decreto nº 10.047/2019), cria uma gigantesca e unificada base de dados dos cidadãos. Ainda não se sabe a finalidade do compartilhamento nem tampouco como os dados pessoais serão compartilhados pelos órgãos do governo federal – entidades da administração pública direta federal e indireta –, incluindo não só Poder Executivo Federal, como também os demais Poderes.

Autoridades governamentais informam que as medidas previstas nos dois decretos facilitarão o acesso dos brasileiros a serviços governamentais. Segundo Luís Felipe Monteiro, Secretário de Governo Digital do Ministério da Economia, o compartilhamento de dados dos cidadãos facilitará o acesso de determinada informação pelos órgãos públicos e o Cadastro Base do Cidadão (CBC) vai otimizar o relacionamento das pessoas com as instituições públicas, evitando que elas tenham que preencher novos cadastros para lidar com cada instituição[37].

Certamente, a digitalização e a desburocratização dos serviços públicos são necessárias e tais medidas representam uma antiga reivindicação da população brasileira. Contudo, em que pesem as boas intenções externadas pelos representantes governamentais, os Decretos nº 10.046/2019 e nº 10.047/2019 – que deveriam regulamentar matéria disciplinada pela LGPD – encontram-se em descompasso com pontos cruciais e com os pilares e paradigmas normativos da legislação de proteção de dados, bem como, com as normas constitucionais atinentes à matéria.

Ademais, a estrutura de governança do Decreto nº 10.046, que cria o Comitê Central de Governança de Dados, não é recomendável, haja vista que tal Comitê

[35] Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D10046.htm>. Acesso em: 30 de outubro de 2019.
[36] Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D10047.htm>. Acesso em: 30 de outubro de 2019.
[37] Disponível em: <http://agenciabrasil.ebc.com.br/geral/noticia/2019-10/governo-regulamenta-uso-de-dados-de-cidadaos-e-cria-cadastro-unificado>. Acesso em: 31 de outubro de 2019.

Central não será composto pela Autoridade Nacional de Proteção de Dados – ANPD nem tampouco por representantes de empresas e de entidades da sociedade civil. Como afirma Rafael Zanatta, "isso vai na contramão do que as leis sobre a relação entre direito e tecnologia exigem em relação à governança. Tanto o Marco Civil da Internet (Lei nº 12.485/2014) quanto a LGPD apontam isso ao exaltar a participação de estruturas multissetoriais, como o Comitê Gestor da Internet (CGI.Br) e o Conselho Nacional de Proteção de Dados (CNPD)".[38]

Alguns especialistas consideram que pode estar sendo criada uma *ferramenta de vigilância estatal extremamente poderosa*, que inclui informações pessoais básicas, mas também dados laborais e biométricos, *como "características biológicas e comportamentais mensuráveis da pessoa natural que podem ser coletadas para reconhecimento automatizado, tais como a palma da mão, as digitais dos dedos, a retina ou a íris dos olhos, o formato da face, a voz e a maneira de andar"* (art. 2º, II, do Decreto nº 10.046/2019 – grifo meu).

A voracidade incessante de alguns Estados/Governos por informações pessoais costuma ser justificada e defendida por inúmeros argumentos, de cunho sociopolítico e econômico, como, por exemplo: a criação de melhores políticas de segurança pública e o combate à criminalidade (ex.: adoção de tecnologias de reconhecimento facial/biométrico); a implementação de medidas para uma administração pública mais eficiente (ex.: os modelos de cidades-inteligentes); a otimização dos serviços públicos (ex.: medidas de facilitação para abertura de empresas, sistemas de reclamações e ouvidoria pública etc.)

Essa voracidade estatal pelos nossos dados nos conduz à reflexão sobre o sinistro panorama traçado por Frank Pasquale, no renomado livro *The Black Box Society* – The Secret Algorithms that control Money and Information,[39] em que o autor demonstra que os dados pessoais dos cidadãos têm sido utilizados através de nebulosas parcerias de empresas com os governos para a criação do chamado "*One-Way Mirror*", possibilitando que esses agentes saibam tudo dos cidadãos, sem qualquer transparência, em um sistema obsessivo de monitoramento e vigilância de cada passo (físico ou digital), consolidando uma *sociedade de vigilância* ("*surveillance society*").

Como desenvolveremos nos tópicos seguintes deste parecer, a criação de tais normas através dos Decretos nº 10.046 e nº 10.047/2019 não foi precedida de uma discussão pública prévia envolvendo a sociedade civil, os empresários e os órgãos multissetoriais (como o Comitê Gestor da Internet). Além disso, não foram lançadas campanhas de conscientização e de alerta à população em relação às novas políticas públicas que estão sendo implantadas.

A grandiosidade da empreitada gera fundadas suspeitas de riscos de vazamentos de dados pessoais, haja vista que os decretos disciplinam a centralização

[38] Disponível em: <http://agenciabrasil.ebc.com.br/geral/noticia/2019-10/governo-regulamenta-uso-de-dados-de-cidadaos-e-cria-cadastro-unificado>. Acesso em: 31 de outubro de 2019.
[39] PASQUALE, Frank. *The Black Box Society* – The Secret Algorithms That Control Money and Information. Harvard University Press, 2015.

de 51 bases de cadastro nacionais (CPF, Renavam, CNPJ, FGTS, Folha Salarial do Seguro-Desemprego, Sisu, ProUni, Fies, Prontuário Eletrônico dos Pacientes do SUS etc.), além das novas bases (Base Integradora e Base Temática) compostas por atributos biográficos e por atributos biométricos de todos os brasileiros.

Temos a destacar inúmeros outros aspectos preocupantes: o não atendimento aos princípios de proteção de dados pessoais estabelecidos pela LGPD; a facilitação de programas futuros que estabeleçam convênios de acesso a empresas privadas que se conectariam a essas informações através do cadastro centralizado; problemas sérios de governança, posto que o Comitê Central de Governança previsto no Decreto nº 10.046/2019 é composto apenas por órgãos do governo federal, sem qualquer participação de entidades da sociedade civil; a ausência da Autoridade Nacional de Proteção de Dados nas decisões e na supervisão do Comitê Central de Governança, em descompasso com as normas da LGPD e criando a possibilidade de decisões contraditórias de órgãos governamentais superpostos, decisões estas que poderão ser extremamente prejudiciais para os titulares de dados pessoais.

Como alertam Juliano Maranhão e Ricardo Campos, a criação do Cadastro Base do Cidadão, através de decreto presidencial, livremente compartilhado entre órgãos públicos, *"vai na contramão da salvaguarda de garantias e direitos da proteção de dados moderna"*. Desta forma, *"coloca o indivíduo como refém da obscuridade pela qual a burocracia estatal pode interligar uma variedade de dados pessoais coletados em diversas esferas da administração pública, em nome de uma maior eficiência para políticas públicas que não foram previamente esclarecidas"*. Eis o alerta mais importante dos respeitados juristas*: "coloca em risco a própria democracia liberal, no contexto da sociedade da informação, ao ignorar a divisão informacional de poderes, pavimentando, com isso, o caminho para a criação de um indomável Leviathan 4.0"*.[40]

4- CONFLITOS DOS DECRETOS Nº 10.046/2019 E Nº 10.047/2019 EM FACE DAS NORMAS CONSTITUCIONAIS E LEGAIS – PRESSUPOSTOS METODOLÓGICOS

O reconhecimento da força normativa das disposições constitucionais é o primeiro marco do direito constitucional contemporâneo, fazendo com que os princípios e regras da Constituição tenham aplicabilidade direta e imediata.

O segundo marco do novo direito constitucional é a expansão da jurisdição constitucional, a qual, como afirma Luís Roberto Barroso, se materializou, no Brasil, na "atribuição do direito de propositura de ações constitucionais diretas a um longo elenco de entidades, o que permitiu fossem levadas ao Supremo Tribunal Federal algumas das grandes questões do debate político, social e moral contemporâneo".[41]

[40] Disponível em: <https://www.jota.info/paywall?redirect_to=//www.jota.info/opiniao-e-analise/artigos/a-divisao-informacional-de-poderes-e-o-cadastro-base-do-cidadao-18102019>. Acesso em 28 de novembro de 2019.

[41] BARROSO, Luís Roberto. *O Novo Direito Constitucional Brasileiro* - Contribuições para a Construção Teórica e Prática da Jurisdição Constitucional no Brasil. Belo Horizonte: Fórum, 2013, p. 31.

E o terceiro marco do direito constitucional contemporâneo é a nova interpretação constitucional, que determina que toda interpretação jurídica deve ser feita à luz da Constituição, dos seus valores e dos seus princípios.

A partir dessas considerações, analisaremos os pontos conflitantes dos Decretos em face da legislação constitucional e infraconstitucional relacionada à proteção de dados e à privacidade, apontando os riscos e descompassos que desestabilizam o sistema de proteção de dados erigido no nosso ordenamento jurídico.

Levaremos em conta as seguintes premissas hermenêuticas:

a) A noção de posição hierárquico-normativa dos Decretos analisados em face das normas constitucionais e legais. Em regra, a existência de hierarquia dos decretos em face das leis no ordenamento jurídico impede que uma regulamentação através de norma infralegal (decretos, portarias e outras normas infralegais) viole uma norma legal, visto que, *na hierarquia dos atos normativos, a lei se sobrepõe ao decreto.*

b) No entanto, a Constituição consagrou espaços de atuação originária do Poder Executivo, a chamada *"reserva de administração"* dos regulamentos autônomos, na qual a lei não pode invadir o espaço normativo dessa "reserva".

c) Nos pontos colidentes com a proteção do direito fundamental à proteção de dados, discutiremos se os Decretos em tela se valem da chamada "reserva de administração", haja vista que *eventual conflito entre normas é resolvido através da interpretação constitucional e da submissão das normas hierarquicamente inferiores às normas que estão no ápice do ordenamento jurídico, ou seja, no texto constitucional.*

5- CONCEITOS JURÍDICOS E REGRAS ESPECÍFICAS DO DECRETO Nº 10.046/2019 CONFLITANTES COM A CONSTITUIÇÃO FEDERAL E COM A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

Neste parecer, optamos por concentrar o nosso estudo no Decreto nº 10.046/2019, diante das suas flagrantes inconsistências e deficiências regulatórias, que suscitam importantes questionamentos em relação à privacidade e à proteção de dados, apresentando conflitos com a legislação constitucional e infraconstitucional. Por conseguinte, deixamos para uma futura avaliação o Decreto nº 10.047/2019.

Deve-se registrar que, com base no entendimento de que o ato normativo do Poder Executivo extrapolou o seu poder regulamentar, foram apresentados, no Congresso Nacional, de acordo com a nossa pesquisa, três Projetos de Decreto Legislativo com o objetivo de sustar o Decreto nº 10.046/2019.[42]

O primeiro Projeto de Decreto Legislativo para a sustação do Decreto nº 10.046/2019 foi o PDL nº 661/2019, de autoria do Deputado Federal André Figueiredo (PDT-CE), o segundo PDL, de nº 673/2019, de autoria do Deputado Federal Orlando Silva (PCdoB-SP), relator da LGPD e da PEC 17/2019. Quanto ao terceiro PDL, de nº

[42] O art. 49, inciso V, da Constituição Federal atribui competência exclusiva ao Congresso Nacional para sustar os atos normativos do Poder Executivo que exorbitem do poder regulamentar.

675/2019, foi apresentado pelo Deputado Federal Ivan Valente (PSOL-SP), na Câmara dos Deputados. Ambos estão nas fases iniciais de tramitação do processo legislativo.

Congratulamo-nos com os Parlamentares que apresentaram os PDLs no Congresso Nacional. Esperamos que tenham uma rápida tramitação e que atinjam o seu objetivo principal. Isto também evitaria que outros entes federativos – os Estados, Municípios e o Distrito Federal – seguissem o mesmo "modelo regulatório" da União, editando decretos com idênticas bases autoritárias e controversas deficiências regulatórias.

Por outro lado, a vigência imediata do Decreto nº 10.046/2019 possibilita a sua contestação através da via judicial, visto que qualquer indivíduo com os seus direitos ameaçados ou violados por força da aplicação do Decreto nº 10.046/2019 poderá buscar no Poder Judiciário a tutela jurisdicional específica. Entretanto, cabe às entidades da sociedade civil organizada ligadas à proteção de dados pessoais e à privacidade discutir outras medidas cabíveis e com alcance mais amplo.

5.1- NATUREZA JURÍDICA DO DECRETO Nº 10.046/2019 E O CONTROLE DE CONSTITUCIONALIDADE: TRATA-SE DE UM DECRETO REGULAMENTAR OU ESTAMOS DIANTE DE UM LEGÍTIMO DECRETO AUTÔNOMO?

No âmbito de atuação desta Comissão de Privacidade e Proteção de Dados da OAB/RJ, coube-nos a avaliação de quais seriam os mecanismos e as ações cabíveis para a defesa dos direitos fundamentais à proteção de dados e à privacidade dos titulares de dados pessoais eventualmente ameaçados por força do Decreto nº 10.046/2019, bem como, quais dispositivos específicos do referido decreto deveriam ser invalidados (ou reconfigurados).

Deve-se considerar que é pacífico no Supremo Tribunal Federal o entendimento de que é inadequado questionar ato regulamentar (ex. decretos, portarias) por meio de ação direta de inconstitucionalidade (ADI), no sentido de que o questionamento de ilegalidades do ato regulamentar deve ser feito no confronto com a legislação infraconstitucional (perante o juízo/Tribunal competente). Isto porque o decreto regulamentar é um ato normativo secundário, sujeito ao controle de constitucionalidade apenas pela via difusa, sendo incabível o controle concentrado de constitucionalidade.

Neste ponto, é necessário examinar a natureza jurídica do Decreto nº 10.046/2019: trata-se de um singelo decreto regulamentar ou estamos diante de um decreto autônomo?[43] Sendo um decreto autônomo, ele entra em conflito com normas legais e/ou com normas constitucionais?

O Decreto nº 10.046/2019 dispõe, no seu Preâmbulo, que se vale das atribuições conferidas no art. 84, *caput*, incisos IV e VI, alínea "a", da Constituição Federal. *Por conseguinte, o Decreto nº 10.046/2019 ingressa no campo dos decretos autônomos, que não se confundem com o mero decreto regulamentar, porque o decreto autônomo*

[43] O decreto autônomo é uma espécie normativa que se limita às hipóteses de organização e funcionamento da administração federal, quando não implicar aumento de despesa nem criação ou extinção de órgãos públicos.

decorre diretamente do poder normativo que lhe é conferido pela própria Constituição, possuindo efeitos análogos ao de uma lei ordinária.

Desta forma, o decreto autônomo previsto no art. 84, VI, alínea "a", da Constituição (como é o caso do Decreto nº 10.046/2019) é ato normativo primário, pois inova no mundo jurídico, é dotado de abstração e generalidade. Em razão disso, esta espécie normativa sujeita-se ao controle difuso e também ao controle concentrado de constitucionalidade.

É importante consignar que o Decreto nº 10.046/2019, no seu preâmbulo, refere-se à Lei de Acesso à Informação (Lei nº 12.527/2011), à Lei nº 13.444/2017 (Lei que cria a Identificação Civil Nacional) e *ao Capítulo IV da Lei nº 13.709/2018 (o capítulo da LGPD que disciplina o Tratamento de Dados Pessoais pelo Poder Público).* Neste aspecto, o Decreto nº 10.046/2019 *parece* exercer o papel de decreto regulamentar. Contudo, ao examinar melhor as disposições do Decreto nº 10.046/2019, verificamos que o ato do Poder Executivo não regulamenta fielmente o Cap. IV da LGPD. Ao contrário, o Decreto *contraria diversos dispositivos da Lei Geral de Proteção de Dados Pessoais. Portanto, este decreto assume as feições de decreto autônomo, pois inova no mundo jurídico, criando novas regras contrárias à própria LGPD, que ainda se encontra em* vacatio legis.

Nesse sentido, o Decreto nº 10.046/2019 não só provoca desafios interpretativos; na realidade, ele invade competência normativa que não lhe é outorgada pela Constituição Federal, viola direitos fundamentais e, na prática, estabelece regras que sugerem uma quase-exclusão do Poder Público Federal do arcabouço normativo da Lei Geral de Proteção de Dados Pessoais.

Frise-se que *para o STF é irrelevante a forma do ato para se identificar se um ato normativo é primário ou secundário***.** O que importa, para a Corte Constitucional, é o *verdadeiro conteúdo normativo do ato.* Neste sentido, temos um importante precedente – um autêntico *leading case* – no julgamento da ADI (medida cautelar) nº 1.748-RJ, de relatoria do Ministro Sidney Sanches, proposta pelo Procurador-Geral da República em face de Ato Normativo.

O supracitado ato normativo era o Aviso nº 227/1997 expedido pelo Corregedor-Geral de Justiça do Estado do Rio de Janeiro, que instituía a *inconciliável figura do Promotor de Justiça* ad hoc. Foi acolhido o argumento da representação da Associação do Ministério Público do Estado do Rio de Janeiro, destacando-se que a forma escolhida pelo Corregedor – *Aviso* – nenhuma relevância tinha para qualificar o ato ou para impedir que este fosse tido como ato normativo primário. *Desta forma, entendeu o STF: a forma é irrelevante. O que importa é o conteúdo do ato; se genérico e abstrato, será considerado* ato normativo primário*, mesmo que se autodenomine decreto regulamentar, portaria ou aviso.*

Pelo acima exposto, conclui-se que o Decreto nº 10.046/2019 assume a figura de um ato normativo primário e exorbita sobremaneira os poderes normativos previstos no art. 84, inciso IV e VI, a*, da Constituição Federal. Ademais, viola os dispositivos previstos no art. 5º, X, XII, XIV e XXXIII da Carta Magna, desafiando a propositura dos remédios de controle*

concentrado de constitucionalidade pelos órgãos, agentes e instituições legitimados, entre os quais o Conselho Federal da Ordem dos Advogados do Brasil (art. 103, VII, da CF).

5.2- REVOGAÇÃO DO DECRETO Nº 8.789/2016 E AS INCOMPATIBILIDADES DO DECRETO Nº 10.046/2019 COM OS FUNDAMENTOS E PRINCÍPIOS DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

Cumpre destacar, com base no disposto no §1º do art. 4º da LGPD, que os *dados pessoais coletados para fins exclusivos de segurança pública, defesa nacional, segurança do Estado e em atividades de investigação e repressão de infrações penais* – excluídos da incidência da LGPD, nos termos do art. 4º, inciso III, e que serão objeto de uma legislação específica[44] – *devem ter o seu processo de tratamento feito com a observação do devido processo legal, dos princípios gerais de proteção e dos direitos do titular previstos na lei geral.*

Nos termos do art. 26 da LGPD, o uso compartilhado de dados pessoais pelo Poder Público deve atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios de proteção de dados pessoais elencados no art. 6º da lei:

> I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
>
> II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
>
> III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
>
> IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
>
> V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
>
> VI - transparência: garantia, aos titulares, de informações claras,

[44] Insta salientar que o Presidente da Câmara dos Deputados, Rodrigo Maia, nomeou uma Comissão de Juristas destinada a elaborar um anteprojeto de lei para regulamentar o tratamento de dados pessoais no âmbito da segurança pública, investigações penais e repressão de infrações penais, conforme a previsão da *LGPD*. A referida Comissão será presidida pelo Ministro Nefi Cordeiro, do STJ. Disponível em: <https://www.migalhas.com.br/quentes/316055/comissao-de-juristas-vai-criar-anteprojeto-para-tratamento-de-dados-pessoais-por-orgaos-de-seguranca>. Acesso em: 10 de dezembro de 2019.

> precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
>
> VII - segurança: utilização de medidas 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 difusão;
>
> VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
>
> IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
>
> X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

O Cadastro Base do Cidadão, instituído pelo Decreto nº 10.046/2019, prevê a inclusão de quaisquer dados das diversas bases temáticas, institucionalizando um cadastro unificado. A regulamentação anterior, disciplinada pelo revogado Decreto nº 8.789/2016, já era passível de críticas por carregar lacunas e possíveis riscos à privacidade e à proteção de dados dos cidadãos.[45]

O Decreto nº 8.789/2016 dispunha, no seu art. 8º, que a solicitação de acesso a bases de dados de outros órgãos públicos federais (apenas do Poder Executivo Federal) se daria por uma solicitação formal específica e fundamentada, com diversos requisitos, como a identificação do solicitante e do seu endereço eletrônico institucional, a descrição clara dos dados objeto da solicitação e da periodicidade da necessidade de utilização, bem como a descrição das finalidades de uso dos dados, além de medidas atinentes à segurança de acesso à base de dados. Além disso, previa, no seu art. 3º, hipóteses de liberação automática do compartilhamento de dados cadastrais e, no caso de dados individualizados não cadastrais, o compartilhamento seria realizado de acordo com as necessidades dos órgãos interessados (art. 5º).

Esse decreto de 2016 fora divulgado como medida de modernização da administração pública e simplificação dos mecanismos de promoção da eficiência na gestão pública, o que gera perplexidade diante dos resultados inexpressivos desse ato normativo.

Entretanto, em outubro de 2019, com o mesmo discurso do endereçamento dos graves problemas das bases de dados governamentais, das fraudes e das

[45] É importante destacar que os dados protegidos por sigilo fiscal sob gestão da Secretaria da Receita Federal estavam excluídos desse compartilhamento sob a égide do Decreto nº 8.789/2016 e continuam excluídos, nos termos do §2º do art. 1º do Decreto nº 10.046/2019.

inconsistências na execução das políticas públicas, entrou em vigor o Decreto nº 10.046/2019, trazendo *maiores riscos à privacidade e à proteção de dados* (em comparação ao Decreto nº 8.789/2016).

Ademais, o cenário jurídico de 2019 já era diverso do cenário de 2016, visto que a Lei Geral de Proteção de Dados Pessoais fora sancionada em 2018, aguardando apenas o término do período da *vacatio legis*, e a PEC 17/2019 encontrava-se em votação no Congresso Nacional. *Esse período de* vacatio *da LGPD destina-se à adequação dos setores público e privado, de forma que, até agosto de 2020, todo o sistema de proteção de dados insculpido pela LGPD seja o norte e a referência para a elaboração de políticas públicas e para as regulamentações setoriais necessárias.*

É importante consignar que concordamos com a construção, no Brasil, de um sistema *seguro e legítimo* de identidade digital do cidadão, tema que já foi objeto de uma lei específica (Lei nº 13.444/2017). E o fato de o governo federal pretender dar efetividade ao Capítulo IV da LGPD, que cuida do tratamento de dados pelos órgãos públicos, seria extremamente positivo, caso se cumprissem adequadamente as normas da LGPD.

Entretanto, ainda que o art. 3º, inciso I, do Decreto nº 10.046/2019 preveja, entre as diretrizes elencadas para o compartilhamento de dados que se observe o disposto na LGPD, verifica-se, no detalhamento das demais normas do decreto, que *as regras adotadas para o compartilhamento de dados pelos órgãos governamentais permitem interligar bases e cruzar dados pessoais sem critérios que sejam conhecidos dos cidadãos, sem informações claras, adequadas e transparentes sobre a realização da coleta e do tratamento, bem como, sobre quem são e como agem os agentes do tratamento.*

Pergunta-se: essa imprevisibilidade seria plenamente justificada para simplificar os serviços públicos, aumentar a eficiência nas prestações públicas, para o combate a fraudes e para reduzir os gastos públicos? *Qual seria o custo dessa política pública em termos de sacrifício dos direitos fundamentais? Poderíamos correr o risco de serem implantados tratamentos e decisões automatizadas baseadas em perfilamento e vigilância em massa? Em tratamento discriminatório e opressivo de minorias? Em repressão de opositores?*

Além disso, a opacidade sobre os agentes de tratamento também trará insegurança jurídica, haja vista que esse tratamento com genéricos objetivos – como o aumento da eficiência na prestação dos serviços públicos – pode facilitar violações aos direitos humanos, como já ocorre na China. Dada a relevância do tema, vale analisar a seguir o sistema de crédito social (*social score*) chinês.

Em livro que aborda o tema do *Big Data*[46], Rodrigo Dias de Pinho Gomes esclarece que a China, com uma população superior a 1 bilhão de habitantes[47], pretende lançar um programa de pontuação, que compreende a gestão de um enorme banco

[46] GOMES, Rodrigo Dias de Pinho. *Big data*: desafios à tutela da pessoa humana na sociedade da informação. 2ª edição. Rio de Janeiro: Lumen Juris, 2019.

[47] 1.382.323.000 habitantes. (UNDATA. China. Disponível em: <http://data.un.org/CountryProfile.aspx?crName=china>. Acesso em: 13 de novembro de 2016).

de dados sobre seus cidadãos[48], alimentado com milhares de informações pessoais, sendo a maioria delas captadas pela internet[49], tais como: histórico de navegação na internet; itens adquiridos em compras; probabilidade de adimplemento de obrigações, entre vários outros, de forma a perfilar e classificar cada um dos chineses.

Tal projeto tem sido objeto de inúmeras críticas[50], visto que vem sendo considerado como a *institucionalização de um verdadeiro* Big Brother *moderno*, pois será obrigatório para toda a população chinesa em 2020, atribuindo a cada indivíduo uma pontuação entre 350 e 950. Esta pontuação ficará vinculada à identidade do cidadão, valendo destacar alguns pontos polêmicos do projeto: o sistema é gerido por duas empresas que administram as redes sociais do país e, portanto, já têm acesso a uma enorme quantidade de dados pessoais sobre os indivíduos e as suas respectivas relações sociais; entre elementos que podem prejudicar a pontuação de um cidadão estão a manifestação de opiniões políticas, incluindo as manifestações de seus amigos, que influenciarão não só a sua própria pontuação mas também a pontuação das pessoas com as quais possuem relacionamentos (familiares, colegas, amigos); a compra de determinados bens melhora a pontuação do indivíduo, enquanto outros bens comprados poderão reduzi-la; o acesso ao sistema permitirá que qualquer interessado verifique a pontuação de qualquer pessoa.

Na realidade, o intuito velado do sistema de *social score* chinês passa a ser a existência de um sistema de controle da moralidade social: *"Critics say China's internet is fast becoming a laboratory where big data meets big brother, where the march of technology combined with profit-driven private companies, authoritarian politics and weak civil liberties is creating a toxic cocktail"*.

Considerando este exemplo assombroso de má utilização do *Big Data* para práticas que claramente violam direitos da personalidade, renova-se a atenção

---

48 "*China's plan to organize its society relies on 'big data' to rate everyone*." (DENYER, Simon. *China's plan to organize its society relies on 'big data' to rate everyone.* The Washington Post, Oct. 2016. Disponível em: <https://www.washingtonpost.com/world/asia_pacific/chinas-plan-to-organize-its-whole-society-around-big-data-a-rating-for-everyone/2016/10/20/1cd0dd9c-9516-11e6-ae9d-0030ac1899cd_story.html>. Acesso em: 13 nov. 2016). Tradução livre: "O plano da China para organizar sua sociedade depende do "*big data*" para avaliar todos".

49 "*Harnessing the power of big data and the ubiquity of smartphones, ecommerce and social media in a society where 700 million people live large parts of their lives online, the plan will also vacuum up court, police, banking, tax and employment records. Doctors, teachers, local governments and businesses could additionally be scored by citizens for their professionalism and probity*." (DENYER, Simon. China wants to give all of its citizens a score: and their rating could affect every area of their lives. Independent, Oct. 2016. Disponível em: <http://www.independent.co.uk/news/world/ asia/china-surveillance-big-data-score-censorship-a7375221.html>. Acesso em: 13 de novembro de 2016. Tradução livre: "Aproveitando o poder do *big data* e a onipresença de smartphones, *e-commerce* e redes sociais em uma sociedade onde 700 milhões de pessoas vivem grandes partes de suas vidas on-line, o plano também irá captar dados judiciais, policiais, bancários, fiscais e registros de emprego. Médicos, professores, governos locais e empresas também poderiam ser avaliados pelos cidadãos por seu profissionalismo e probidade".

50 "*´This is the most staggering, publicly announced, scaled use of big data I've ever Seen', says Michael Fertik, a Silicon Valley entrepreneur and author of The Reputation Economy.*" (OBBEMA, Fokke; VLASKAMP, Marije; PERSSON, Michael. *China rates its own citizens* – Including online behaviour. The Volkskrant, Apr. 2015. Disponível em: <http://www.volkskrant.nl/buitenland/china-rates-its-own-citizens-including-online>. Acesso em: 13 de novembro de 2016.

necessária ao estabelecimento de mecanismos legais consentâneos com o atual estado da tecnologia, em que esta possa ser compatibilizada e harmonizada com a privacidade e a proteção de dados pessoais. Neste sentido, a LGPD foi elaborada com estes específicos mecanismos legais, haja vista que prevê a possibilidade de compartilhamento de dados para a execução de políticas públicas com a observância de normas que salvaguardam os direitos fundamentais**.** *Conclui-se que, de forma alguma, a LGPD admite a integração* a priori *dos dados em um cadastro unificado e gigantesco.*

Ademais, a LGPD obriga, no seu art. 23, que as pessoas jurídicas de direito público interno previstas no parágrafo único do art. 1º da Lei de Acesso à Informação observem, em relação ao tratamento de dados pessoais que estão sob a sua guarda, que este se dê para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, desde que:

I- Sejam informadas as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos;

II- Seja indicado um encarregado quando realizarem operações de tratamento de dados pessoais.

O art. 4º do Decreto nº 10.046/2019 prevê a criação de 3 níveis de compartilhamento, de acordo com sua confidencialidade (amplo, restrito e específico), ficando a cargo do "gestor de dados" a categorização do nível de compartilhamento. A opacidade desta regra é preocupante e o nível de governança desse sistema padece de grande subjetividade. E esse "gestor de dados" foge completamente às figuras do controlador e do operador, previstas na LGPD. Outrossim, o "gestor de dados" também não se compatibiliza com a figura do *encarregado*, conforme o disposto no art. 23, inciso III, da lei geral.

É importante ressaltar que *interligar bases de dados e permitir o seu cruzamento sem critérios que sejam devidamente esclarecidos enfraquece o direito à autodeterminação informativa*. Os titulares dos dados serão privados de informações claras, adequadas e facilmente acessíveis sobre a coleta e sobre a realização do tratamento dos dados. O cidadão estaria obrigado a aceitar a coleta estatal de um dado pessoal para uma determinada finalidade (como a execução de uma determinada política pública), com base no art. 7º, inciso III, da LGPD. Contudo, estaria vivendo em um regime de insegurança, posto que o dado coletado mediante aquela finalidade poderia ser utilizado seguidamente para uma outra finalidade, sem o seu conhecimento. Isso viola a LGPD e estaria em desconformidade com as regras e os padrões internacionais de proteção de dados.

Melhor explicando: a LGPD prevê que o tratamento e compartilhamento de dados pela administração pública, entre as hipóteses elencadas nas bases legais do

art. 7º, restringe-se aos dados necessários para a execução daquela determinada política pública, não para uma cadeia indefinida e indeterminada de finalidades inadequadas e/ou obscuras.

Entendemos que qualquer compartilhamento de dados pessoais sem critérios claros, sem a finalidade adequada (e bem definida) e com preocupante opacidade quanto aos procedimentos adotados estaria vedado pela LGPD e violaria os dispositivos constitucionais atinentes à privacidade e à proteção de dados.

5.3- CRIAÇÃO DE NOVOS CONCEITOS DE DADOS PESSOAIS ALHEIOS À LGPD: AMPLIAÇÃO DA COLETA DE DADOS PESSOAIS SENSÍVEIS E CRIAÇÃO DE UM SISTEMA DE VIGILÂNCIA MASSIVO?

Causou perplexidade entre os especialistas em proteção de dados a inserção, no Cadastro Base do Cidadão criado pelo Decreto nº 10.046/2019, de *conceitos estranhos à LGPD* no que diz respeito aos dados pessoais, como atributos biográficos e biométricos. Os atributos biométricos, em uma *relação não taxativa* (art. 2º, II, do Decreto), incluem a retina ou a íris dos olhos, o formato da face, a voz e a maneira de andar. *Desta forma, amplia-se sobremaneira a extensão dos dados cadastrais que serão coletados e tratados pelos órgãos governamentais.*

O conteúdo dos dados biográficos inclui dados inexistentes nas anteriores bases cadastrais e de conceituação extremamente vaga, como "fatos da sua vida" (art. 2º, I, do Decreto nº 10.046/2019) e "grupo familiar". Atualmente o conceito de família já não se limita à família biológica, mas inclui a família socioafetiva, o que, por si só, amplia a base de dados biográficos dos cidadãos.

Como a chamada *Biometria Comportamental* está em franca expansão, sendo especialmente incorporada pelas tecnologias de monitoramento, temos um indício de que a coleta desses dados poderá ser massiva, com o argumento de que o Estado está adotando políticas públicas para evitar fraudes e para promover maior segurança para a população. *Essas políticas deveriam ser adotadas com maior grau de transparência, sob pena de se criar um estado de permanente vigilância, com drásticas consequências para os direitos individuais.*

Além disso, as chamadas *base integradora e base temática (art. 2º, incisos VI e VII do Decreto nº 10.046/2019), que integrarão os atributos biográficos previstos no art. 2º, I, e os atributos biométricos, provocam indagações sobre o contexto em que ocorrerão o tratamento e a utilização dessas novas bases e o cruzamento desses dados*, especialmente diante do avanço dos sistemas de tratamento automatizado e dos mecanismos de decisão automatizada decorrentes do crescimento exponencial da inteligência artificial, como o reconhecimento facial. Tais informações podem ser utilizadas para um controle político intenso dos cidadãos, típico de regimes totalitários.

Outrossim, uma grande preocupação surge do *descompasso entre as normas do Decreto nº 10.046/2019 e o tratamento que a LGPD disciplina para a coleta dos dados pessoais sensíveis*, que estão elencados no art. 5º, inciso II: 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.

Como são conceitos novos, criados pelo Decreto nº 10.046/2019, surge outra pergunta: *serão considerados dados pessoais sensíveis esses atributos biográficos e biométricos que integrarão as bases integradora e temática? Serão observadas as regras específicas do art. 11 da LGPD, que exigem procedimentos diferenciados para a coleta e o tratamento de dados sensíveis? Será dada publicidade à dispensa do consentimento, nos termos do §2º do art. 11 e do inciso I do art. 23 da LGPD?*

5.4- RISCOS IMEDIATOS RELATIVOS À SEGURANÇA DA INFORMAÇÃO: A LGPD SERÁ RELEGADA A UM CARÁTER MERAMENTE DECORATIVO?

O vazamento de dados é um tema que tem chamado cada vez mais atenção, não apenas em âmbito nacional, mas especialmente na esfera internacional, e esse foi um dos maiores impulsos para a criação de lei específica sobre o tema. Como é do conhecimento geral, uma das exigências para o ingresso do Brasil na OCDE (Organização para a Cooperação e Desenvolvimento Econômico) e em outras entidades internacionais importantes, como a Eurojustice e a Europol, foi a aprovação de uma lei geral de proteção de dados, mas é necessário que o nosso país demonstre que a LGPD não terá um caráter meramente decorativo. Todos os países que ingressam na OCDE devem cumprir requisitos técnicos para se adequar aos princípios defendidos pela Organização, que incluem a proteção dos dados pessoais nas transações comerciais.

A pesquisa anual da IBM em parceria com o Instituto Ponemon (*Cost of a Data Breach*) indicou que o Brasil é o quarto país no *ranking* de registros de dados vazados, com 26.523 registros, atrás apenas de Oriente Médio (38.800), Índia (35.636) e EUA (32.434). No ano de 2019, apenas em relação a bases públicas (tanto em órgãos públicos, como em serviços privados exercidos por delegação do Poder Público), ocorreram inúmeros vazamentos de dados pessoais em órgãos públicos, como nos DETRANs de diversos estados e nos sistemas do Governo do Distrito Federal.

Nos Cartórios do Registro Civil das Pessoas Naturais em São Paulo, a situação tomou um tom ainda mais dramático. Segundo matérias jornalísticas, foram vazados 988 mil arquivos, sendo que um único deles teria 381 mil certidões de nascimento com informações de cerca de 1 milhão de pessoas. E o mais assustador: essas informações ficaram dois meses *online*, à disposição de quem quisesse copiá-las.[51]

O próprio *CTIRGov*, órgão do governo federal, possui estatísticas assombrosas com milhares de registros acerca de incidentes cibernéticos relacionados à segurança dos sistemas de computação ou das redes de computadores em órgãos ou entidades dos Poderes da União, dos Estados e dos Municípios.[52]

[51] Disponível em: <https://noticias.uol.com.br/cotidiano/ultimas-noticias/2019/10/29/falha-de-cartorios-expoe-dados-de-ao-menos-1-milhao-de-pais-maes-e-filhos.htm>. Acesso em: 03 de novembro de 2019.
[52] Disponível em: <www.ctir.gov.br>. Acesso em: 03 de novembro de 2019.

Buscando uma outra experiência sem precedentes de centralização dos dados de milhões de cidadãos, verificamos o que ocorreu na Índia, em que um conjunto de vazamentos de dados biométricos e outras informações pessoais expôs cerca de 130 milhões de pessoas ao risco de fraudes e outros crimes digitais. De acordo com o *Centre for Internet and Society* (CIS) de Bangalore, brechas em quatro bancos de dados gerenciados pelas autoridades indianas revelaram na internet os números de identificação não somente dos cidadãos indianos, mas também de qualquer pessoa que more e trabalhe na Índia. Nesse país oriental, cada pessoa tem um número de identificação, do sistema Aadhaar, que é um código com 12 dígitos. Esses códigos são mantidos em um banco de dados central da *Unique Identification Authority of India*, onde ficam ligados a dados biométricos que combinam a leitura de íris e as impressões digitais. Segundo a organização CIS, esses vazamentos são sintomáticos de um dano significativo e potencialmente irreversível à privacidade dos indianos.

Assim como se procura justificar a implantação do Cadastro Base do Cidadão, na Índia, a criação do sistema Aadhar foi enaltecida como um sistema que aplicaria a biometria para evitar fraudes e garantiria o acesso facilitado a programas de saúde, educação e assistência pública. Entretanto, as controvérsias sobre questões relativas à privacidade surgiram desde o início e a segurança do sistema foi questionada diante da escala gigantesca da empreitada.[53] Os resultados desastrosos mostram os danos à privacidade e à proteção de dados sendo descortinados. Contudo, muitos pesquisadores e jornalistas indianos que identificaram brechas no descomunal projeto de identidade nacional da Índia alegam que foram perseguidos por agências do governo e estão sendo acusados criminalmente por causa do seu trabalho investigativo.[54]

Em conclusão, as vulnerabilidades de um banco de dados gigantesco, como aquele disciplinado pelo Decreto nº 10.046/2019, sugerem imensos riscos de vazamentos e de incidentes de segurança que podem comprometer irreversivelmente a privacidade e a proteção de dados dos cidadãos brasileiros.

5.5- SUPERPOSIÇÃO DE ÓRGÃOS E PROBLEMAS DE GOVERNANÇA, DE FISCALIZAÇÃO E DE *ENFORCEMENT*

O Decreto nº 10.046 entrou em vigor na data da sua publicação. No art. 21, institui o Comitê Central de Governança, cujos membros seriam indicados em até 15 dias, ou seja, até o dia 24 de outubro de 2019. O Comitê é integrado apenas por funcionários da administração direta, sem qualquer previsão de composição multissetorial. *Todavia, em questões relacionadas à tecnologia, a experiência brasileira (e internacional) mostra que o multissetorialismo é a melhor prática*. A participação no Comitê (com garantia de assento) do setor privado, da sociedade civil organizada e da comunidade técnica garantiria que as questões relacionadas entre direito e

[53] Disponível em: <https://www.tecmundo.com.br/seguranca-de-dados/116338-vazamento-dados-biometricos-expoe-130-milhoes-risco-fraude-india.htm>. Acesso em: 04 de novembro de 2019.
[54] Disponível em: <https://br.reuters.com/article/worldNews/idBRKBN1H10VF-OBRWD>. Acesso em: 04 de novembro de 2019.

tecnologia tivessem uma visão multidisciplinar. A LGPD e o Marco Civil da Internet (Lei nº 12.485/2014) apontam para essa composição, com o Conselho Nacional de Proteção de Dados e Privacidade (CNPD) e o Comitê Gestor da Internet (CGI.Br).

Além disso, não ficou evidenciado se esse órgão terá alguma vinculação com a Autoridade Nacional de Proteção de Dados – ANPD, o que causa grande preocupação, visto que, sendo um comitê que definirá questões fundamentais para o sistema jurídico de proteção de dados pessoais, a ausência de interlocução nessa matéria poderá produzir decisões contraditórias e até mesmo desastrosas para os titulares de dados pessoais.

Mais grave: além de não ficar clara a vinculação com a ANPD, há evidências de que haverá um eventual conflito de atribuições ou mesmo uma superposição de atribuições entre a ANPD e o Comitê Central de Governança, diante das antinomias de normas jurídicas, como se vê a seguir.

O art. 55-K da LGPD prevê que a aplicação das sanções previstas na lei compete exclusivamente à ANPD *e suas competências prevalecerão, no que se refere à proteção de dados pessoais, sobre as competências correlatas de outras entidades ou órgãos da administração pública.*

Nos termos do parágrafo único do art. 55-K, a ANPD articulará sua atuação com outros órgãos e entidades com competências sancionatórias e normativas afetas ao tema de proteção de dados pessoais *e será o órgão central de interpretação desta Lei e do estabelecimento de normas e diretrizes para a sua implementação.*

O art. 21 do Decreto nº 10.046/2019 dispõe que fica instituído o *Comitê Central de Governança de Dados, a quem compete deliberar sobre diversas matérias que deveriam ser objeto de deliberação da ANPD.* Além disso, o art. 26 do Decreto prevê que *as controvérsias no compartilhamento de dados entre órgãos e entidades públicas federais solicitantes de dados e o gestor de dados serão decididas pelo Comitê Central de Governança de Dados, com a possibilidade de consulta ao Comitê Interministerial de Governança, sem qualquer previsão de consulta à ANPD.*

E o fato de a Autoridade Nacional de Proteção de Dados ainda não ter sido nomeada causa maior insegurança jurídica aos titulares de dados pessoais, visto que *compete à ANPD solicitar aos órgãos e às entidades do poder público informações sobre o âmbito e a natureza dos dados e outros detalhes do tratamento realizado, podendo emitir parecer técnico complementar para garantir o cumprimento da LGPD. Com a autonomia técnica e decisória assegurada à ANPD pelo art. 55-B, há uma grande expectativa de que a sua atuação técnica possa garantir a efetiva implementação da lei, sendo de vital importância medidas como a solicitação de relatórios de impacto à proteção de dados pessoais e a sugestão da adoção de padrões e de boas práticas para os tratamentos de dados pessoais pelo Poder Público (art. 31 da LGPD).*

Atribuições fundamentais da ANPD, relacionadas aos seus poderes de fiscalização e de *enforcement*, previstas no art. 31 da LGPD, incluem, ainda, a averiguação de violações em decorrência do tratamento de dados pessoais por órgãos públicos e a adoção de medidas cabíveis para fazer cessar a violação, *inclusive as sanções*

administrativas previstas nos incisos I, IV, V, VI, X, XI e XII do art. 52, que podem ser aplicadas às entidades e aos órgãos públicos, sem prejuízo do disposto no Estatuto do Servidor Público, na Lei de Improbidade Administrativa e na Lei de Acesso à Informação (nova redação do §3º do art. 52 da LGPD, após a derrubada, pelo Congresso Nacional, dos vetos presidenciais).

É lícito assegurar que competências específicas do Conselho Nacional de Proteção de Dados e da Privacidade contribuirão positivamente para a atuação da ANPD, auxiliando na formulação das diretrizes estratégicas e para a elaboração da Política Nacional de Proteção de Dados Pessoais e da Privacidade, com especial atenção aos dados pessoais tratados pelo Poder Público.

5.6- DA NECESSIDADE DE HARMONIZAÇÃO DAS NORMAS ATINENTES À PROTEÇÃO DE DADOS EM CONSONÂNCIA COM AS REGRAS DE TRANSFERÊNCIA INTERNACIONAL DE DADOS

Atualmente, praticamente todas as empresas atuam com a coleta e o tratamento de dados pessoais, seja no seu cadastro de clientes, seja na análise de grandes quantidades de informações para extrair resultados, seja na gestão da folha de pagamentos; melhor dizendo, os dados estão em todos os setores da economia. Considerando que hoje, para as novas tecnologias e para os atuais modelos de negócios, as fronteiras geográficas estão desaparecendo, é fundamental que estes dados circulem pelo mundo, não só nos diversos servidores, mas em sistemas de armazenamento em nuvem e de *cloud computing*.

É importante mencionar que a LGPD, em seu artigo 33, a exemplo da GDPR, exige, para a *licitude da transferência internacional de dados*, que o outro país ou organismo envolvido em uma relação contratual proporcione *grau de proteção de dados pessoais adequado ao previsto na lei. Quando isto não for possível, caberá ao controlador oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos na Lei, o que representa maiores gastos para as empresas envolvidas*.

Note-se que *atualmente o Brasil não dispõe do reconhecimento do nível de proteção adequado pela comunidade europeia,* o que significa dizer que as empresas europeias que realizam transferência internacional de dados com o Brasil enfrentam um custo *muito superior em relação a negócios com empresas de outros países da América do Sul* como a Argentina e o Uruguai, que atualmente são "homologados" na União Europeia neste quesito.

Na dura realidade enfrentada pelo empresariado local, a ausência de reconhecimento de elevado nível de proteção de dados no Brasil gera enormes custos para as empresas brasileiras e também para as empresas estrangeiras que querem estabelecer negociações com as nossas empresas, na medida em que esta situação implica aumento de exigências e burocracias para a comprovação das garantias de cumprimento dos princípios de proteção de dados, dos direitos do titular e do regime

geral de proteção de dados previstos na LGPD e na GDPR, encarecendo bastante os produtos e serviços brasileiros.

Isto significa dizer que o Decreto nº 10.046/2019 poderá representar um *indesejado obstáculo para que o Brasil obtenha o tão desejado reconhecimento formal dos europeus como país com nível adequado de proteção de dados. Neste diapasão, a almejada certificação está seriamente colocada em risco, porquanto as regras atinentes à tutela de dados pessoais não se mostrarão efetivas com a nova sistematização introduzida pelo decreto, sistemática esta que possibilita, em tese, a violação de direitos fundamentais dos cidadãos brasileiros.*

Como já destacado anteriormente, as Diretrizes para a Proteção da Privacidade e dos Fluxos Transfronteiriços de Dados Pessoais ("Diretrizes sobre a Privacidade") foram adotadas como Recomendação do Conselho da OCDE em apoio aos três princípios comuns aos países membros da OECD: democracia pluralista, respeito aos direitos humanos e economias de mercado aberto. Os países Membros da OCDE devem estabelecer procedimentos e instituições legais e administrativas efetivas e comprometidas com a proteção da privacidade e da liberdade pessoal em matéria de dados pessoais.

Não se pode retroceder em relação a conquistas no campo dos direitos fundamentais, na medida em que, além de todos os pontos destacados, temos hoje a oportunidade de implantar uma legislação alinhada às melhores práticas internacionais, crucial para o desenvolvimento do ambiente de negócios e para as transferências internacionais, a fim de promover a melhora de competitividade das empresas brasileiras.

5.7- A IRRESPONSABILIDADE ADMINISTRATIVA, SENDO FONTE DE INSEGURANÇA JURÍDICA E GERANDO IMPACTOS ECONÔMICOS NEGATIVOS

A Lei nº 13.874/2019 proclama, em seu preâmbulo, a "Declaração de Direitos de Liberdade Econômica", estabelecendo garantias de livre mercado e alterando diversas leis, entre elas o Código Civil, a CLT, a Lei das Sociedades Anônimas e a Lei dos Registros Públicos.

A Lei nº 13.874/19 também inseriu *a análise do impacto regulatório* como medida importante a ser adequadamente tratada. O art. 5º determinou a realização da análise do impacto regulatório antes da edição e da alteração de atos normativos de interesse geral de agentes econômicos ou de usuários dos serviços prestados. Essa análise deve considerar os *possíveis efeitos do ato normativo para verificar a razoabilidade do seu impacto econômico.*

Outrossim, a Lei nº 13.874/19 combate expressamente o *abuso do poder regulatório*, assim descrito, em síntese, como aquele que redige enunciados que impeçam ou retardem a inovação e a adoção de novas tecnologias, processos ou modelos de negócios.

Ademais, cumpre informar que o Brasil caiu 15 posições no *Doing Business 2020*, *ranking* do Banco Mundial que analisa a regulamentação do ambiente de negócios.

Entre 190 economias, o país caiu da 109º para 124º colocação, aproximando-se da posição que ocupou durante 2017 e 2018. Nações como México (60º), Índia (63º) e África do Sul (84º) estão à nossa frente. São analisadas as cidades de São Paulo e do Rio de Janeiro e os dados são relativos ao mês de maio de 2019.

A despeito dos contornos mais ou menos incisivos da atuação dos agentes econômicos, *a criação do Cadastro Base do Cidadão*, nos termos definidos pelo Decreto nº 10.046/2019*, ensejará insegurança jurídica e produzirá negativas repercussões econômicas que afastarão os investimentos no Brasil.*

Nestes termos, a edição do Decreto nº 10.046/2019, de forma descoordenada e sem a devida consonância com a LGPD, configura-se uma situação *sui generis* em que o Administrador Público propõe uma concentração de dados pessoais em um único cadastro unificado, em um ambiente inóspito, *sem a existência de processos de conformidade legal com a proteção de dados pessoais, podendo gerar danos aos titulares de dados pessoais, caracterizando-se, em tese, a responsabilidade civil objetiva das pessoas jurídicas de direito público, nos termos do art. 37, §6º, da Constituição Federal, amparada na teoria do risco administrativo.*

Em conclusão, diante da ausência total de elementos concretos de processo de conformidade legal com a proteção de dados pessoais, a implantação do Cadastro Base do Cidadão, nos moldes criados pelo Decreto nº 10.046/2019, colocaria em risco todas as atividades de atração de investimentos, prejudicando o ambiente de negócios, assim como, possibilitaria atração de riscos de responsabilização para os entes públicos e para os gestores públicos.

6- PRECEDENTES DO SUPREMO TRIBUNAL FEDERAL: RESTRIÇÕES AO COMPARTILHAMENTO DE DADOS ENTRE ÓRGÃOS DA ADMINISTRAÇÃO PÚBLICA E VEDAÇÃO AO "CONSTITUCIONALISMO ABUSIVO"

6.1- DECISÕES QUE RESTRINGEM O COMPARTILHAMENTO DE DADOS ENTRE ÓRGÃOS DA ADMINISTRAÇÃO PÚBLICA (ÁREAS ADMINISTRATIVA E CÍVEL)

O Supremo Tribunal Federal tem dois precedentes importantes para o balizamento da questão atinente ao compartilhamento dos dados entre órgãos públicos. Toda a argumentação exposta neste parecer e os precedentes que serão apresentados podem levar ao questionamento da constitucionalidade de dispositivos do Decreto nº 10.046/2019, impedindo-se a criação do tal cadastro unificado como foi concebido no ato normativo do Poder Executivo Federal.

No Mandado de Segurança MS 36150 MC/DF, impetrado pelo Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira – INEP contra o Acórdão 2609/2018 do Tribunal de Contas da União – TCU, o *INEP insurge-se contra a decisão do TCU, proferida nos autos do Processo TCU 032.908/2017-2, que determinou a entrega de dados individualizados do Censo Educacional e do ENEM para auditoria do Programa Bolsa Família.*

No supracitado mandado de segurança, o Relator, Ministro Luís Roberto Barroso, concede a liminar com fundamento no art. 5º, incisos X, XIV e XXXIII, da Constituição Federal, e na Lei nº 12.527/2011 (Lei de Acesso à Informação), que asseguram o sigilo de dados pessoais. Além disso, o Ministro baseia-se no princípio da finalidade, posto que considera que as informações prestadas ao INEP pelos jovens estudantes são fornecidas para o atendimento de uma determinada finalidade declarada no ato da coleta de dados, não podendo ocorrer a transmissão desses dados para outro órgão público para atendimento de finalidade diversa.

> Ementa: DIREITO CONSTITUCIONAL. MANDADO DE SEGURANÇA. ATO DO TCU. SIGILO ESTATÍSTICO. DADOS INDIVIDUALIZADOS DO ENEM E DO CENSO ESCOLAR. 1. Mandado de segurança impetrado pelo Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira – INEP contra acórdão do TCU que determinou a entrega de dados individualizados do Censo Escolar e do ENEM para auditoria do Programa Bolsa Família. 2. O art. 5º, X, XIV e XXXIII, da CF/1988, e a Lei nº 12.527/2011 – Lei de acesso à informação – asseguram o sigilo de dados pessoais. A divergência quanto ao dever de sigilo do INEP sobre os dados requisitados pelo TCU é matéria sujeita à reserva de jurisdição, não cabendo ao órgão de controle externo decidir sobre a caracterização de ofensa à garantia constitucional. 3. As informações prestadas ao INEP são fornecidas por jovens estudantes para o atendimento de uma finalidade declarada no ato da coleta dos dados e sob a garantia de sigilo das informações pessoais. É plausível a alegação de que a transmissão desses dados para finalidade diversa: (i) subverte a autorização daqueles que concordaram em prestar as declarações; e (ii) coloca em risco a capacidade do INEP de pesquisar e monitorar políticas públicas. 4. Além disso, o fornecimento dos dados requisitados pelo TCU esvaziaria o objeto da impetração, o que justifica o deferimento da liminar. 5. Perigo de dano demonstrado diante da iminência de incidência de multa e da aplicação de sanção de afastamento da autoridade responsável pela entrega dos dados. 6. Liminar concedida.[55]

O segundo precedente do STF que restringe o compartilhamento de dados entre órgãos públicos encontra-se na decisão liminar proferida pela Ministra Cármen Lúcia na Medida Cautelar em Suspensão de Liminar nº 1103 SP, na qual o Instituto Brasileiro

[55] Disponível em: http://www.stf.jus.br/portal/jurisprudencia/listarJurisprudencia.asp?s1=%28%28INEP+E+TCU%29%28%28ROBERTO+BARROSO%29%2ENORL%2E+OU+%28ROBERTO+BARROSO%29%2ENPRO%2E+OU+%28ROBERTO+BARROSO%29%2EDMS%2E%29%29+NAO+S%2EPRES%2E&base=baseMonocraticas&url=http://tinyurl.com/w45c2o7 Acesso em: 11 de novembro de 2019.

de Geografia e Estatística – IBGE insurge-se contra uma decisão da Quarta Turma do Tribunal Regional Federal da Terceira Região, proferida na Apelação Cível nº 000568 7 -25.2012.4.03.6 l 08/SP, em que são partes o Ministério Público Federal e o IBGE.

Ao decidir a favor do IBGE, a Relatora prestigia a proteção ao sigilo estatístico, alegadamente indispensável às atividades desempenhadas pelo IBGE e à garantia da fidelidade dos dados estatísticos pelos quais subsidiada a elaboração de políticas públicas destinadas ao desenvolvimento socioeconômico e regional, objetivo fundamental da República (art. 3º da Constituição da República):

> (...) Nesse cenário, o cumprimento da determinação judicial de prestar as informações requisitadas pelo Ministério Público Federal, mediante o afastamento excepcional do sigilo estatístico, surge como grave precedente e parece ganhar contornos extravagantes.
>
> Tanto não induz, por outro lado, reconhecer caráter absoluto ao sigilo de dados estatístico levantados pelo IBGE, que pode vir a ceder por determinação judicial quando as circunstâncias do caso concreto assim impuserem.
>
> Não fosse apenas isso a recomendar a suspensão dos efeitos da decisão contrastada, a execução provisória da obrigação de fazer, mediante o fornecimento da identificação pessoal postulada pelo Ministério Público, não poderia ser revertida no futuro, conduzindo ao prejuízo da presente suspensão de liminar e dos eventuais recursos que, porventura, venham a ser dirigidos pelo IBGE aos Tribunais Superiores.
>
> 9. Assim, o exame preliminar e superficial da causa conduz a reconhecer que o afastamento do sigilo estatístico imposto pela decisão contrastada dispõe de potencialidade lesiva à ordem pública, por abalar a confiança daqueles que prestam as informações aos entrevistadores do IBGE, comprometendo a fidelidade e veracidade dos dados fornecidos e, por conseguinte, a própria finalidade daquele Instituto, a subsidiar a elaboração de políticas públicas em benefício da sociedade.
>
> 10. Pelo exposto, defiro liminarmente o requerimento para suspenderem-se os efeitos da decisão proferida pelo Tribunal Regional Federal da Terceira Região no julgamento da Apelação Cível nº 000568725.2012.4.03.6108/SP (art. 12, §1º, da Lei nº 7.347/1985, art. 4º da Lei nº 8.437/1992 e art. 297 do Regimento Interno do Supremo Tribunal Federal).[56]

[56] Disponível em: <portal.stf.jus.br/processos/downloadPeca.asp?id=311747237&ext=.pdf>. Acesso em: 11 de novembro de 2019.

6.2- OS RISCOS DO "CONSTITUCIONALISMO ABUSIVO", QUE PROMOVE RETROCESSO DEMOCRÁTICO E VIOLAÇÃO A DIREITOS FUNDAMENTAIS

Em dezembro de 2019, o Supremo Tribunal Federal, através de importante decisão monocrática do Ministro Luís Roberto Barroso, restabeleceu o mandato dos membros do CONANDA – Conselho Nacional dos Direitos da Criança e do Adolescente, que haviam sido destituídos imotivadamente através do Decreto nº 10.003/2019. Este Decreto do Presidente da República alterou as normas sobre a constituição e o funcionamento do Conanda e promoveu a destituição imotivada de todos os seus membros, no curso regular dos seus mandatos.

A decisão do Ministro Barroso foi proferida nos autos da Medida Cautelar na Arguição de Descumprimento de Preceito Fundamental 622 / Distrito Federal, proposta pela então Procuradora-Geral da República, Raquel Dodge, que afirmou que a norma impugnada esvaziou a participação da sociedade civil no Conselho, em violação aos princípios da democracia participativa (art. 5º, CF), da proteção à criança e ao adolescente (art. 227, CF) e de vedação ao retrocesso institucional (art. 1º, *caput* e III; art. 5º, XXXVI e §1º; art. 60, §4º, CF).

Insta salientar que a decisão em tela faz um extenso arrazoado do chamado *"constitucionalismo abusivo",* fenômeno danoso que vem atingindo os regimes democráticos, cuja expressão foi cunhada por David Landau[57]. Essa forma de constitucionalismo utiliza institutos de origem democrática para ceifar o pluralismo em um determinado país, "adaptando" os próprios mecanismos formais do sistema democrático para minar a democracia e os direitos fundamentais. Com muita propriedade, aduz o Ministro Relator:

> (...) os retrocessos democráticos, no mundo atual, não decorrem mais de golpes de estado com o uso das armas. Ao contrário, as maiores ameaças à democracia e ao constitucionalismo são resultado de alterações normativas pontuais, aparentemente válidas do ponto de vista formal, que, se examinadas isoladamente, deixam dúvidas quanto à sua inconstitucionalidade. Porém, em seu conjunto, expressam a adoção de medidas que vão progressivamente corroendo a tutela de direitos e o regime democrático.
>
> Esse fenômeno tem recebido na ordem internacional diversas denominações, entre as quais: "constitucionalismo abusivo", "legalismo autocrático" e "democracia iliberal". Todos esses conceitos aludem a experiências estrangeiras que têm em comum a atuação de líderes carismáticos, eleitos pelo voto popular, que, uma vez no poder, modificam o ordenamento jurídico, com o propósito de assegurar a sua permanência no poder. O modo

[57] LANDAU, David. *Abusive constitucionalism*. University of California Davis Law Review, Estados Unidosm vol. 47, nº 1, 2013, p. 189-260.

> de atuar de tais líderes abrange: (i) a tentativa de esvaziamento ou enfraquecimento dos demais Poderes, sempre que não compactuem com seus propósitos, com ataques ao Congresso Nacional e às cortes; (ii) o desmonte ou a captura de órgãos ou instituições de controle, como conselhos, agências reguladoras, instituições de combate à corrupção, Ministério Público etc.; (iii) o combate a organizações da sociedade civil, que atuem em prol da defesa de direitos no espaço público; (iv) a rejeição a discursos protetivos de direitos fundamentais, sobretudo no que respeita a grupos minoritários e vulneráveis – como negros, mulheres, população LGBTI e indígenas; (v) o ataque à imprensa, sempre que leve ao público informações incômodas para o governo.[58]

Deve-se ressaltar que as alterações normativas promovidas pelo Decreto nº 10.003/2019, à semelhança das alterações normativas previstas no Decreto nº 10.046/2019, sinalizam que a edição dos referidos decretos ocorreu no contexto em que havia uma impossibilidade – constitucional e legal –, de diminuição e/ou supressão dos direitos fundamentais.

Neste parecer, demonstramos que, através da edição do Decreto nº 10.046/2019, criou-se uma aparente legalidade para, em verdade, serem promovidas alterações profundas na Lei Geral de Proteção de Dados Pessoais que solapam os direitos dos titulares de dados pessoais e promovem a quase-exclusão do Poder Público Federal do arcabouço normativo da LGPD. Devem-se observar os limites necessários para que o poder normativo conferido pela Constituição ao Chefe do Poder Executivo Federal não seja um instrumento oposto ao que disciplina a própria Lei Fundamental da República.

Em conclusão, destacamos que os atos discricionários do Presidente da República, ao exercer a direção superior da administração pública federal e ao regulamentar e dispor sobre a organização e o funcionamento dos órgãos do Poder Executivo, *encontram limites na Constituição da República e nas leis federais. A inobservância desses limites autoriza o Poder Judiciário a revisá-los porque, nesta hipótese, estamos diante de um juízo quanto à constitucionalidade e à legalidade dos atos do Chefe do Poder Executivo.*

Reiterando as palavras do Ministro Roberto Barroso, entendemos *que cabe à Corte Constitucional, como a corte de mais alta hierarquia em matéria constitucional, estar atenta a alterações normativas que, a pretexto de dar cumprimento à Constituição, em verdade se inserem em uma estratégia mais ampla de concentração de poderes abusiva e distorcida, de violação a direitos fundamentais e de retrocesso democrático, como entendemos ser exatamente o que resulta do Decreto nº 10.046/2019, nos termos expostos neste parecer.*

[58] Disponível em: <https://www.jota.info/wp-content/uploads/2019/12/efddc66cf24522b5830084f2ee8430ca.pdf>. Acesso em: 15 de janeiro de 2020.

7- CONCLUSÃO

Inicialmente, entendemos que devem ser olvidados todos os esforços junto ao Congresso Nacional para que o Decreto nº 10.046/2019 seja suspenso através da iniciativa dos Projetos de Decreto Legislativo mencionados neste parecer – os PDLs 661, 673 e 675/2019 –, haja vista as incongruências, deficiências regulatórias e violações a disposições constitucionais relativas à privacidade e à proteção de dados pessoais que o Decreto nº 10.046/2019 apresenta.

Concomitantemente, consideramos fundamental que sejam adotadas medidas políticas e jurídicas destinadas à cobrança da nomeação e instalação da Autoridade Nacional de Proteção de Dados. É importante destacar que, enquanto não se instala a ANPD, temos um decreto presidencial em vigor há mais de três meses, atribuindo a um órgão monossetorial (somente com integrantes do governo federal e sem qualquer participação dos órgãos multissetoriais) a competência relativa à tomada de decisões importantes na esfera da privacidade e da proteção de dados dos brasileiros, adultos ou crianças. Essas atribuições previstas no Decreto nº 10.046/2019 conflitam-se com as atribuições da própria ANPD, criam insegurança jurídica e podem ocasionar riscos e/ou danos aos titulares de dados pessoais.

No tocante à medida judicial sugerida neste parecer, conclui-se que o Decreto nº 10.046/2019 assume a figura de um ato normativo primário que exorbita os poderes normativos previstos no art. 84, inciso IV, da Constituição Federal e viola os dispositivos previstos no art. 5º, incisos X, XII, XIV e XXXIII, e art. 84, incisos IV e VI, a, da Carta Magna, desafiando a propositura de Arguição de Descumprimento de Preceito Fundamental (ADPF) ou de Ação Direta de Inconstitucionalidade (ADI) pelo Conselho Federal da Ordem dos Advogados do Brasil, legitimado nos termos do art. 103, VII, da Constituição Federal.

Este é o parecer,

S.M.J.

Rio de Janeiro, 30 de janeiro de 2020.

LUCIA MARIA TEIXEIRA FERREIRA

OAB/RJ 207.385

Membro da Comissão de Proteção de Dados e Privacidade da OAB/RJ