A Administração Pública na Lei Geral de Proteção de Dados

Luciano Elias Reis

Rafael Knorr Lippmann

1 Introdução

Restando poucos meses para a entrada em vigor da Lei Geral de Proteção de Dados – LGPD brasileira,[1] já se constata uma elevada atenção da sociedade a seu respeito. Cursos e debates têm sido propostos, ao tempo em que a academia, como é seu papel, vem apresentando ampla produção literária a respeito dos mais diversos aspectos relacionados à LGPD.

Entretanto, pouco tem se tratado a respeito da Administração Pública neste cenário, constatação que soa até mesmo paradoxal, tendo em vista que, mundialmente, foi ela, a Administração Pública, a grande mola propulsora das primeiras discussões e propostas legislativas para regulação do tratamento de dados pessoais.[2]

---

[1] A Lei nº 13.709, de 14 de agosto de 2018, que nos termos de sua ementa estabelece a "Lei Geral de Proteção de Dados Pessoais", foi publicada no Diário Oficial da União de 15 de agosto de 2018, prevendo na redação originária o seu art. 65, II, que entraria em vigor "24 (vinte e quatro) meses após a data de sua publicação", à exceção de seus arts. 55-A, 55-B, 55-C, 55-D, 55-E, 55-F, 55-G, 55-H, 55-I, 55-J, 55-K, 55-L, 58-A e 58-B, que, nos termos de seu art. 65, I, vigem desde 28 de dezembro de 2018. *Contudo*, em 2020, houve, por meio da Lei nº 14.010, a inclusão do artigo 65, I-A, para determinar o início da vigência a partir do dia 1º de agosto de 2021 quanto aos artigos 52, 53 e 54, assim como a Medida Provisória nº 959, que prescreveu o termo inicial de vigor para 3 de maio de 2021 aos demais artigos, ou seja, substituindo aquela intenção inicial de vinte e quatro meses.

[2] Como relata Simson Garfinkel, em 1965, o *Bureau of Budget* norte-americano propôs a criação do *National Data Center*, um gigantesco banco de dados que unificaria perante a Administração Pública as informações dos cidadãos constantes dos bancos do fisco, previdência social, polícia, etc. (GARFINKEL, Simson. *Database Nation.* Sebastopol: O'Rilley. 2001). Apesar de nunca ter sido levado a efeito, a proposição do *National Data Center* é apontada como o despertar da sociedade à forma como instituições, tanto públicas como privadas, obtêm, armazenam, divulgam, transmitem e eliminam dados pessoais, tendo sido rejeitada, dentre outros motivos e como aponta Danilo Doneda, pelo temor das consequências que a centralização, nas mãos do

O objetivo deste ensaio é, sem a pretensão de exaurir o debate, traçar os contornos do tratamento dado à Administração Pública na LGPD e apresentar uma reflexão crítica a seu respeito, destacando avanços, apontando possíveis lacunas e apresentando sugestões voltadas ao equacionamento adequado da relação entre proteção de dados e Administração Pública à luz do Estado Democrático de Direito.

2 Dados pessoais e a Administração Pública

A preocupação com o tratamento de dados pessoais por terceiros não é novidade. Há décadas e em diversos países o tema vem recebendo grande atenção social e legislativa. Tome-se o exemplo de Espanha[3] e Portugal,[4] países que tipificaram em suas Constituições e, bem assim, como verdadeira garantia fundamental o direito à proteção dos dados pessoais, inclusive aqueles tratados com o emprego da informática.

No Brasil, embora o assunto não seja propriamente uma novidade, a roupagem a ele atribuída pela LGPD é, efetivamente, *nova*. Isso porque, até o advento da Lei nº 13.709/2018, o direito à proteção de dados pessoais era visto como uma espécie de decorrência, de desdobramento do direito à intimidade e da inviolabilidade de correspondência, telefônica e fiscal, dentre outros pilares extraídos do rol de garantias fundamentais constitucionais.[5]

Estado, das informações de todos os cidadãos daquele país, poderiam trazer (DONEDA, Danilo. *Da privacidade à proteção de dados pessoais.* Rio de Janeiro: Renovar. 2006, p. 189).

[3] No inciso 4 de seu artigo 18, disciplinador do "derecho a la intimidad" e da "inviolabilidad del domicilio", a Constituição da Espanha dispõe que "La Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos".

[4] O art. 35, da Constituição portuguesa, entabula em seus incisos as premissas básicas ao tratamento de dados com o amparo da informática, estabelecendo em seu inciso 1 que "todos os cidadãos têm o direito de acesso aos dados informatizados que lhes digam respeito, podendo exigir a sua rectificação e actualização, e o direito de conhecer a finalidade a que se destinam, nos termos da lei".

[5] "A proteção de dados pessoais no ordenamento brasileiro, até recentemente, não se estruturava em um complexo normativo unitário. A Constituição brasileira contempla o problema da informação inicialmente através das garantias à liberdade de expressão e do direito à informação, que deverão eventualmente ser confrontados com a proteção da personalidade e, em especial, com o direito à privacidade. Além disso, a Constituição considera invioláveis a vida privada e a

Se, por um lado, essa perspectiva já concebia o direito à proteção de dados pessoais, de outro deixava-o desguarnecido de tratamento adequado, dando margem a lacunas e distorções.

É nessa medida que a LGPD brasileira, que surge na denominada quarta onda do direito à proteção de dados, dá nova conformação ao direito à proteção de dados, garantindo não só a tão aclamada autodeterminação informativa[6] àquele cujos dados serão entregues aos cuidados de terceiros como – e especialmente – estabelecendo uma verdadeira *cadeia de responsabilidades* àqueles que terão sob sua posse os dados atinentes à personalidade dos cidadãos.[7]

Diante desse panorama, é quase que imediata a constatação de que a Administração Pública assume relevante posição na temática dos dados pessoais. Se, como dito, desde seu nascedouro a preocupação mundial com o tratamento de dados esteve relacionada ao Estado, hoje ela é ainda mais marcante.

Desde o nascimento de uma pessoa, a partir do registro civil no Cartório de Pessoas Naturais ou Jurídicas, passando pelo cadastro nos órgãos de saúde, do trabalho,

---

intimidade (art. 5º, X), veja-se especificamente a interceptação de comunicações telefônicas, telegráficas ou de dados (artigo 5º, XII), bem como instituiu a ação de *habeas data* (art. 5º, LXXII), que basicamente estabelece uma modalidade de direito de acesso e retificação de dados pessoais" (DONEDA, Danilo. A autonomia do direito fundamental de proteção de dados. *In:* SOUZA, Carlos Affonso; MAGRANI, Eduardo; SILVA, Priscilla (Coord.). *Lei Geral de Proteção de Dados.* São Paulo: RT, 2019, p. 27).

[6] Expressão que ganhou notoriedade a partir de julgamento levado efeito pelo Tribunal Constitucional alemão em 1983, no qual a Corte reconheceu a existência de um direito fundamental de envolvimento do indivíduo em todo o processo de tratamento de seus dados por terceiros, não apenas na "etapa inicial" consistente na anuência de fornecê-los ou não. Sobre o tema: MENDES, Laura Schertel. *Habeas data* e autodeterminação informativa. *Revista brasileira de direitos fundamentais & justiça*, v. 12, n. 39, p. 185-216, jul./dez. 2018.

[7] "(...) a efetividade da proteção de dados não reside mais apenas em ampliar o controle do indivíduo mas também em atribuir responsabilidade a toda a cadeia de agentes de tratamento de dados pelos riscos do processamento de informações" (MENDES, Laura Schertel. A lei geral de proteção de dados pessoais: um modelo de aplicação em três níveis. *In:* SOUZA, Carlos Affonso; MAGRANI, Eduardo; SILVA, Priscilla (Coord.). *Lei Geral de Proteção de Dados.* São Paulo: RT, 2019, p. 42).

fiscais, previdenciários, etc., a Administração Pública é responsável pela coleta, armazenamento, tratamento, transmissão e arquivamento de dados de toda a população.

Some-se a isso o fato de que, ao contrário do que ocorre com instituições privadas, perante as quais a pessoa, ao menos em tese, tem a opção de fornecer ou não os seus dados, ante a Administração Pública o fornecimento de informações é *compulsório*, implicando a omissão na configuração de um ilícito.[8]

Portanto, não é exagerado afirmar que o Estado tem seus olhos postos sobre todos os aspectos da vida de cada um dos cidadãos que o conformam. Nascimento, grau educacional, bens, movimentações financeiras, laborativas, infrações cometidas, enfim, toda a gama de informações relacionadas à vida e a personalidade, várias delas qualificadas como *sensíveis.*[9]

Sendo o detentor de tamanho volume de informação sobre a população, não é necessário muito refletir para constatar o elevado cuidado necessário ao adequado manuseio dos dados e as catastróficas consequências de sua não observância.

O exemplo trazido por Caitlin Mulholland e Isabella Frajhof é emblemático.[10] Narram as autoras que, no ano de 2016, uma falha no sistema de segurança resultou na ampla divulgação dos dados relacionados a mais de 500.000 pessoas que doaram sangue entre os anos de 2010 e 2016 na Austrália. Dentre as informações descuidadamente abertas, estavam aquelas relacionadas ao comportamento sexual do doador de sangue, dados estes inerentes à intimidade humana e que, bem assim, jamais poderiam ter sido abertamente divulgados.

3 A Administração Pública na LGPD

---

[8] Vide, por exemplo, o art. 1º, inciso I, da Lei nº 8.137/90, que tipifica como crime contra a ordem tributária a omissão de informação à autoridade fazendária.

[9] Nos termos definidos pelo art. 5º, II, da LGPD, considera-se sensível todo "dado pessoal dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural".

[10] MULHOLLAND, Caitlin; FRAJHOF, Isabella Z. Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da lei geral de proteção de dados (Lei 13.709/18). *Revista de Direitos e Garantias Fundamentais*, Vitória, v. 19, n. 3, p. 159-180, set./dez. 2018. p. 159-160.

Passar de olhos por sobre o texto da LGPD revela, de início, que seu Capítulo IV (arts. 23 a 30) volta-se precipuamente a disciplinar o "tratamento de dados pessoais pelo Poder Público". Grosso modo, esses dispositivos disciplinam critérios de legitimidade (art. 23), abrangência (art. 24), bem como forma e controle do uso compartilhado dos dados (arts. 25 a 30).

Naturalmente, o fato de o Capítulo IV da LGPD dedicar-se à disciplina do tratamento de dados pelo Poder Público não implica a premissa de que as demais disposições da Lei não se apliquem a ele. Do contrário, a sua interpretação sistemática revela que há, em seu texto, diversos princípios e dispositivos que tocam diretamente à seara da Administração Pública.[11]

A seguir, e dentro dos limites deste ensaio, destacam-se aqueles que mais parecem chamar a atenção na relação pragmática entre administração e administrado.

3.1 Princípio da finalidade e a "pertinência temática" no tratamento de dados pessoais

Como referido na introdução deste ensaio, um dos principais motivos que levou à rejeição do plano de criação do *National Data Center* nos Estados Unidos foi o receio de que, a partir dele, o Estado passasse a se utilizar de "informações cruzadas" como forma de subjugar os cidadãos em prol de interesses próprios a ponto de tolher-lhes liberdades e garantias fundamentais.

Imagine-se, por exemplo, o órgão fiscal se utilizando de informações provenientes de processo criminal sigiloso movido em face do contribuinte como forma de compeli-lo ao pagamento de um tributo.

Nesta senda, dentre diversos (e importantíssimos) princípios voltados à proteção de dados que foram tipificados no art. 6º, da LGPD, já em seu inciso I está previsto o da *finalidade*, que, por razões evidentes, é de crucial relevância à gestão de dados praticada pela Administração Pública.

Tanto assim que, mais adiante, o *caput* do art. 23, voltado especificamente à Administração Pública, deixa evidente que o tratamento de dados "deverá ser realizado

[11] Parece ter sido esse, inclusive, o sentido de, mediante o advento da Lei nº 13.853/2019, incluir-se no art. 1º da LGPD um parágrafo único e, nele, prever-se textualmente que "as normas gerais contidas nesta Lei são de interesse nacional e devem ser observadas pela União, Estados, Distrito Federal e Municípios".

para o atendimento de sua finalidade pública", premissa essa reiterada no art. 26, que, ao dispor sobre o uso compartilhado de dados por órgãos do Poder Público, permite-o apenas mediante o atendimento das "finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas".

A cautela empregada no texto legislativo, que num primeiro olhar soaria até como redundância, é absolutamente pertinente e digna de aplausos, por pelo menos dois relevantes motivos.

O primeiro, harmônico com o próprio princípio da *motivação* dos atos administrativos, é o de exigir da Administração a demonstração de necessidade, pertinência e relevância no tratamento de dados de pessoas. Assim, como destaca Danilo Doneda, o tratamento de dados pessoais "deve obedecer à finalidade comunicada ao interessado antes da coleta de seus dados", sendo que a partir dele, em especial quando a utilização da informação se dá pelo Poder Público, é possível "estruturar um critério para valorar a razoabilidade da utilização de determinados dados para uma certa finalidade (fora da qual haveria abusividade)".[12]

O segundo, e ainda mais destacado, é o de que, ao contrário do que se dá com as pessoas de direito privado,[13] à Administração Pública foi garantida pela LGPD a prerrogativa de promover o compartilhamento de dados pessoais *sem o consentimento prévio e expresso do seu titular.*

O art. 26, *caput*, da LGPD autoriza expressamente o compartilhamento *interno* de dados pessoais entre diferentes órgãos da própria Administração, enquanto seu §1º admite o compartilhamento com instituições privadas desde que observados os requisitos entabulados em seus incisos, excetuando o art. 27, nestas hipóteses, a "cláusula geral" de exigência prévia do consentimento do seu titular para compartilhamento dos dados.[14]

---

[12] DONEDA, Danilo. A autonomia do direito fundamental de proteção de dados. *In:* SOUZA, Carlos Affonso; MAGRANI, Eduardo; SILVA, Priscilla (Coord.). *Lei Geral de Proteção de Dados*. São Paulo: RT, 2019, p. 23.

[13] É o que se infere da análise do §5º do art. 7º da Lei, que exige imperativamente do controlador, para que promova o compartilhamento de dados pessoais sob seu poder com outro controlador, "consentimento específico do titular para esse fim".

[14] O art. 29 prevê que a autoridade nacional *poderá* solicitar informações aos entes envolvidos a respeito das operações de tratamento de dados pessoais. Trata-se, a toda vista, de regra de controle bastante branda, pois, além de dar tons de facultatividade à solicitação de informações pela

De toda relevância, pois, a estrita observância do princípio da *finalidade* pela Administração Pública quando promover o tratamento de dados pessoais, exatamente porque, como adverte Laura Schertel Mendes, somente a partir dele é possível "garantir a privacidade contextual, evitando que os dados pessoais sejam utilizados posteriormente para finalidades incompatíveis com aquela para a qual ele foi coletado".[15]

É dizer, independentemente da possibilidade legal expressa de dispensa do consentimento (e, possivelmente, ciência) do interessado, o compartilhamento de dados por um órgão da Administração Pública a outro exige, ainda assim, a estrita observância ao princípio da *finalidade*, de modo que, como regra, a entidade receptora dos dados *não poderá utilizá-los para fim diverso daquele pelo qual foram originariamente fornecidos por seu titular.* Aqui reside a relevância de existir um ato administrativo na forma escrita para que o escopo esteja descrito e atrele as responsabilidades entre os partícipes desse uso compartilhado, inclusive tudo isso já pensando no processo de gestão de riscos que sempre deve ser levado em consideração.

3.2 Controle humano sobre tomada de decisão automatizada

Algo inimaginável há poucos anos, a completa autonomização dos sistemas a partir de tecnologias baseadas em inteligência artificial é uma realidade presente em diversos meios de nossa sociedade,[16] cujo combustível capaz de manter a engrenagem

---

autoridade competente, coloca-a numa posição passiva, sem delimitar qualquer critério objetivo às situações ou elementos que, quando verificados, exigiriam o controle. Adere-se, portanto, à crítica apresentada por Daniel Bucar à sistemática legal: "Diante das amplas possibilidades de compartilhamento de dados pessoais no interior da Administração Pública, a supervisão desenhada para Autoridade Nacional parece ter ficado tímida. Por conta dos potenciais danos desse compartilhamento, deveria a Autoridade, se não autorizar previamente, ser sempre (pelo menos) comunicada ativamente das operações (...)". BUCAR, Daniel. Administração Pública e lei geral de proteção de dados. *In:* SOUZA, Carlos Affonso; MAGRANI, Eduardo; SILVA, Priscilla (Coord.). *Lei Geral de Proteção de Dados.* São Paulo: RT, 2019, p. 163.

[15] MENDES, Laura Schertel. A lei geral de proteção de dados pessoais: um modelo de aplicação em três níveis. *In:* SOUZA, Carlos Affonso; MAGRANI, Eduardo; SILVA, Priscilla (Coord.). *Lei Geral de Proteção de Dados.* São Paulo: RT, 2019, p. 49.

[16] "A IA é empregada, por exemplo, em máquinas de busca, em plataformas de comunicação e robôs, no reconhecimento facial, em equipamentos inteligentes de gestão de tráfego, em decisões administrativas ou jurídicas tomadas de maneira automatizada, em sistemas automatizados de

funcionando é, justamente, o conjunto de dados proveniente dos usuários daquele determinado sistema, permanentemente colhidos, registrados e interpretados pelo "robô", sem qualquer intervenção humana, para os mais diversos fins: selecionar uma rota de trânsito, determinar se o perfil de determinado cidadão se enquadra na categoria "X" ou "Y" ou até mesmo julgar um recurso.[17]

A LGPD, preocupada com essa realidade e sem excluir outros, tratou de municiar o titular dos dados manuseados por terceiros com determinados direitos, ponto este que toca frontalmente à Administração Pública,[18] que, como se extrai da realidade prática,

---

assistência para veículos, no diagnóstico e na terapia médicos, na *smart home* [casa inteligente], em sistemas de produção ciberfísicos (indústria 4.0), mas também na área militar. A ampliação de sistemas de análise e decisão que se baseiam em algoritmos e operam com IA possibilita formas novas de fiscalização e controle do comportamento, mas também novas espécies de ações criminosas". (HOFFMANN-RIEM, Wolfgang. Inteligência artificial como oportunidade para a regulação jurídica. *Revista Direito Público,* Porto Alegre, v. 16, n. 90, p. 12, nov./dez. 2019.

[17] Vide o já célebre caso da Estônia, que, embora ainda como projeto piloto, desenvolveu um sistema de julgamento de ações judiciais por inteligência artificial e, portanto, sem a intervenção da mão de um "juiz humano": https://epocanegocios.globo.com/Tecnologia/noticia/2019/04/estonia-quer-substituir-os-juizes-por-robos.html?utm_source=facebook&utm_medium=social&utm_campaign=post&fbclid=IwAR2lSCcrPka7SxtaeX1yOvyFLm2lAOoFyxTS9qE4g6kP-uewRhCniR0Ivp4, acesso em: 31 jan. 2020. No Brasil, embora não se tenha, ainda, notícia de decisões judiciais proferidas exclusivamente por meio de inteligência artificial, a utilização dessa tecnologia é cada vez mais presente nos Tribunais. Cite-se, como exemplo, os casos do "RADAR" utilizado pelo Tribunal de Justiça de Minas Gerais, que identifica e reúne recursos sobre temas repetitivos e "sugere" ao órgão julgador a tese a ser aplicada conforme jurisprudência já firmada sobre o assunto: https://www.tjmg.jus.br/portal-tjmg/noticias/tjmg-utiliza-inteligencia-artificial-em-julgamento-virtual.htm#.XjP1r2hKhPY, acesso em: 31 jan. 2020; e do "VICTOR", utilizado pelo STF para filtragem dos recursos extraordinários que sobem à Corte a partir dos temas de repercussão geral existentes: http://www.stf.jus.br/portal/cms/verNoticiaDetalhe.asp?idConteudo=388443, acesso em: 31 jan. 2020.

[18] O art. 23, III, LGPD exige, especificamente à Administração Pública, a indicação de um *encarregado* para o tratamento de dados pessoais. A salutar previsão, entretanto, não exclui nem impede que a tomada de decisões seja realizada de forma exclusivamente automatizada, cabendo

vem adotando com entusiasmo a utilização da inteligência artificial no processamento de dados dos cidadãos.[19]

Em seu art. 20, o diploma previu não só a possibilidade de solicitação, pelo interessado, de "revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais" como, e em especial, estabeleceu no §3º desse dispositivo o dever, ao ente prolator da decisão recorrida, de que a revisão seja realizada *por pessoa natural.*[20]

Quanto examinada a partir das relações com a Administração Pública, a norma extraída do texto legal deixa claro o dever imposto ao ente gestor dos dados de, mesmo quando o seu tratamento se dê de forma integralmente informatizada, criação de órgão interno, formado por agentes *físicos* com a finalidade de revisão das decisões tomadas de forma automatizada, sempre que solicitado pelo cidadão interessado.

3.3 Inadequação das sanções legais às infrações praticadas pela Administração Pública

Como forma de estimular o cumprimento de suas diretrizes, em seu art. 52, a LGPD estabeleceu uma série de sanções ao ente que deixar de observar as regras e princípios nela entabulados ao tratamento de dados pessoais.

Esse é, certamente, o ponto mais sensível no que tange à aplicação da LGPD à Administração Pública, tendo em vista que as sanções tipificadas, em especial as mais

---

ao encarregado, nos próprios termos do art. 5º, VIII, da Lei, apenas intermediar a relação entre controlador, titular dos dados e/ou Autoridade Nacional de Proteção de Dados.

[19] Veja-se o exemplo do Estado de Alagoas, no qual a inteligência artificial é responsável não apenas pelo controle e emissão de notas fiscais eletrônicas como, também, por orientar telefonicamente os cidadãos que entram em contato com a Secretaria da Fazenda: http://www.sefaz.al.gov.br/noticia/item/2228-fazenda-usa-sistema-artificial-para-realizar-chamadas-telefonicas-e-interagir-com-os-contribuintes, acesso em: 31 jan. 2020.

[20] Sobre o tema, Patricia Peck Pinheiro~~XXX~~ adverte para a possibilidade – indesejável – de o julgamento continuar a ocorrer pela máquina, sendo apenas elucidado ao titular dos dados através de pessoa humana: "Sendo assim, apesar de a lei prever que o titular pode requerer que seja revisto por uma pessoa natural, muito provavelmente será aplicada a mesma fórmula de análise (algoritmo), mas esclarecido por uma pessoa o processo utilizado para alcançar o resultado" (PINHEIRO, Patricia Peck. *Proteção de dados pessoais* – comentários à Lei 13.709/2018. São Paulo: Saraiva, 2018, p. 83).

severas, foram nitidamente pensadas para incidirem sobre instituições privadas, fazendo pouco ou nenhum sentido quando voltadas à Administração.

É o caso da "multa simples", prevista no inciso II do art. 52 que, bastante enérgica, pode atingir a cifra de R$ 50.000.000,00 contra o infrator das normas previstas na LGPD. Entretanto, como limita o seu texto, a sanção é destinada exclusivamente à "pessoa jurídica, grupo ou conglomerado no Brasil", não se aplicando, pois, às infrações praticadas pela Administração Pública no tratamento de dados pessoais.

Essa premissa, extraível da redação do próprio inciso, é explicitada de forma direta no §3º do dispositivo, ao delimitar que "o disposto nos incisos I, IV, V, VI, X, XI e XII do *caput* deste artigo poderá ser aplicado às entidades e aos órgãos públicos". Chama a atenção, neste caso, a possibilidade de aplicação, à Administração Pública, das sanções tipificadas nos incisos X, XI, e XII do art. 52.

Estes três incisos preveem, respectivamente, como reprimenda à inobservância da LGPD, a suspensão do banco de dados, a suspensão do exercício da atividade de tratamento de dados e a proibição do exercício da atividade de tratamento de dados.

Em que pese a expressa autorização de sua aplicação à Administração Pública, a realidade prática pode tornar inviável ou, então, catastrófica a incidência da sanção em determinados casos.

Imagine-se, por exemplo, que, por uma falha no sistema de segurança, sejam divulgadas pela Receita Federal informações sigilosas constantes de declarações de imposto de renda de parcela da população. Seria possível, neste caso, suspender a utilização do banco de dados (inciso X), ou do exercício da atividade de tratamento de dados (inciso XI), ou mesmo proibir a Receita Federal de tratar dados relacionados aos rendimentos dos contribuintes?

Nitidamente, há um duplo desafio a ser superado: de um lado, dimensionar a aplicabilidade prática das sanções previstas na LGPD à Administração Pública *sem que isso resulte em verdadeiro impedimento da consecução da atividade-fim do órgão estatal* e, de outro, evitar que a inexistência de sanção legalmente adequada venha a gerar a "impunidade" da Administração por ocasião do cometimento de infração à legislação que regula o tratamento de dados pessoais.

3.4 Sanções aos agentes públicos por violação aos dispositivos legais

Conquanto as sanções aplicáveis à "pessoa" do órgão ou da entidade da Administração Pública tenham os seus problemas como esposados anteriormente, convém ressaltar que os agentes públicos, nos termos do artigo 2º da Lei nº 8.429/92, poderão ser sancionados por descumprirem os dispositivos normativos aplicáveis à proteção de dados no Brasil.

Dentre as penalidades passíveis de serem aplicadas, pontuam-se as disciplinares normalmente estabelecidas no Estatuto do Servidor (*v. g.* no âmbito federal pela Lei nº 8.11~~1~~2/90), aquelas relacionadas com a legislação especial de informações públicas (vide artigo 33 da Lei nº 12.527/2011) e as diversas preconizadas na legislação de improbidade administrativa (artigo 12 da Lei nº 8.429/92).

Além dos textos normativos suscitados e que são aludidos no próprio texto da LGPD, há diversos outros diplomas a serem interpretados de maneira sistemática. Tudo isso tem a serventia de externar que as infrações e sanções prescritas na LGPD deverão ser avaliadas em conformidade com o restante do ordenamento jurídico pátrio, não se podendo aplicar uma norma de modo isoladamente. Em especial aos agentes públicos, considerando o volume de dados pessoais a que têm acesso diariamente para o exercício de suas atividades funcionais, o conhecimento da legislação e de seus impactos, a exigência de contratação pelo Poder Público de ferramentais e estruturas técnicas adequadas para o tratamento dos dados e ainda a contínua instrução para acautelar possíveis desvios e para gerenciar riscos e crises, devem ser pauta do 'top five' de toda autoridade superior de órgãos e entidades da Administração Pública.

Conclusão

Do cenário apresentado, vislumbra-se que o protagonismo que a Administração Pública exerce na captação, manutenção, gestão e transmissão de dados não foi integralmente re~~t~~tratado no texto positivado à regulação dessas atividades tão relevantes à consecução do bem-estar social.

Seja como for, à luz do texto da LGPD torna-se inegável a difícil, porém imprescindível, missão que o Poder Público tem de implementar um sistema seguro e confiável de governança digital.[21]

[21] "Governança digital é a prática de estabelecer e implementar políticas, procedimentos e padrões para o desenvolvimento, uso e gestão apropriados da infosfera. (...) Por exemplo, através da governança digital um órgão governamental ou uma empresa poderá: 1) determinar e controlar

Se, de um lado, é inegável o enorme avanço alcançado com o advento da LGPD no tratamento de dados dos cidadãos pela Administração Pública, por outro, em especial no tocante às sanções tipificadas ao ente infrator da lei, alguns de seus dispositivos, quando voltados à mesma Administração, revelam-se inadequados ou mesmo ineficientes.

No entanto, se as sanções para a Administração Pública são por vezes inócuas, o mesmo não se pode asseverar aos agentes públicos, que têm contra si pesadíssimas sanções em caso de afronta à LGPD. Ainda pouco se aborda este viés, porque estão incautos – talvez até pela ignorância e inconsciência dos seus consectários legais ou pela descrença na efetivação da lei.

De todo modo, no presente ensaio, procurou-se analisar criticamente esses pontos e, com o único propósito de trazer o tema ao debate, apresentar possíveis soluções aos entraves que, eventualmente, poderão vir a ser enfrentados tanto pelo cidadão como pelo gestor público por ocasião da entrada em vigor da LGPD.

Referências

BUCAR, Daniel. Administração Pública e lei geral de proteção de dados. *In:* SOUZA, Carlos Affonso; MAGRANI, Eduardo; SILVA, Priscilla (Coord.). *Lei Geral de Proteção de Dados*. São Paulo: RT, 2019.

DONEDA, Danilo. *Da privacidade à proteção de dados pessoais.* Rio de Janeiro: Renovar. 2006.

DONEDA, Danilo. A autonomia do direito fundamental de proteção de dados. *In:* SOUZA, Carlos Affonso; MAGRANI, Eduardo; SILVA, Priscilla (Coord.). *Lei Geral de Proteção de Dados*. São Paulo: RT, 2019.

processos e métodos usados por gestores de dados [*data stewards]* e guardiões de dados [*data custodians*] a fim de melhorar a qualidade, confiabilidade, acesso e segurança dos dados e a disponibilidade de seus serviços; e 2) criar procedimentos eficazes para a tomada de decisões e para a identificação de responsabilidades no que diz respeito a processos relacionados com os dados" (FLORIDI. L. Soft Ethics, the Governance of the Digital and the General Data Protection Regulation. *Philosophical transactions of the royal society*, 2018, A 376. Disponível em: http://dx.doi.org/10.1098/rsta.2018.0081. Acesso em: 31 jan. 2020).

FLORIDI. L. Soft Ethics, the Governance of the Digital and the General Data Protection Regulation. *Philosophical transactions of the royal society,* 2018, A 376. Disponível em: http://dx.doi.org/10.1098/rsta.2018.0081. Acesso em: 31 jan. 2020.

GARFINKEL, Simson. *Database Nation.* Sebastopol: O'Rilley. 2001.

HOFFMANN-RIEM, Wolfgang. Inteligência artificial como oportunidade para a regulação jurídica. *Revista Direito Público,* Porto Alegre, v. 16, n. 90, nov./dez. 2019.

MENDES, Laura Schertel. *Habeas data* e autodeterminação informativa. *Revista brasileira de direitos fundamentais & justiça,* v. 12, n. 39, p. 185-216, jul./dez. 2018.

MENDES, Laura Schertel. A lei geral de proteção de dados pessoais: um modelo de aplicação em três níveis. *In:* SOUZA, Carlos Affonso; MAGRANI, Eduardo; SILVA, Priscilla (Coord.). *Lei Geral de Proteção de Dados.* São Paulo: RT, 2019.

MULHOLLAND, Caitlin; FRAJHOF, Isabella Z. Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da lei geral de proteção de dados (Lei 13.709/18). *Revista de Direitos e Garantias Fundamentais,* Vitória, v. 19, n. 3, p. 159-180, set./dez. 2018.

PINHEIRO, Patricia Peck. *Proteção de dados pessoais* – comentários à Lei nº 13.709/2018. São Paulo: Saraiva, 2018.

REIS, Luciano Elias; LIPPMANN, Rafael Knorr. A Administração Pública na Lei Geral de Proteção de Dados.