



ADMINISTRAÇÃO PÚBLICA ORIENTADA POR DADOS: GOVERNO ABERTO E INFRAESTRUTURA NACIONAL DE DADOS ABERTOS

José Sérgio da Silva Cristóvam¹
Tatiana Meinhart Hahn²

Resumo:

O estudo objetiva, com base na Declaração de Governo Aberto da OGP, do relatório da OCDE e da teoria do conceito de “valor público” de Mark Moore, analisar como a Administração Pública brasileira tem se orientado por dados. Para isso, o primeiro tópico irá abordar conceitos sobre os diferentes tipos de dados que permeiam as funções administrativas no Brasil. Na segunda parte, serão apresentados os fundamentos legais e exemplos práticos sobre governo aberto em curso no país. O método utilizado é o dedutivo e a técnica de pesquisa a bibliográfica, com análise da legislação e jurisprudência relacionadas sobre o tema.

Palavras-chave: Administração Pública; governo aberto; Infraestrutura Nacional de Dados Abertos.

DATA-DRIVEN PUBLIC ADMINISTRATION: OPEN GOVERNMENT AND NATIONAL OPEN DATA INFRASTRUCTURE

Abstract:

The study aims, based on the OGP Open Government Declaration, the OECD report and Mark Moore's theory of the concept of "public value", to analyze how the Brazilian Public Administration has been driven by data. For this, the first topic will address concepts about the different types of data that permeate administrative functions in Brazil. In the second part, the legal grounds and practical examples of open government in progress in the country will be presented. The method used is the deductive and the technique of bibliographic research, with analysis of the legislation and jurisprudence related to the subject.

Keywords: Public Administration; open government; National Open Data Infrastructure.

¹ Professor Adjunto de Direito Administrativo (Graduação, Mestrado e Doutorado) da UFSC. Subcoordenador do PPGD/UFSC. Doutor em Direito Administrativo pela UFSC (2014), com estágio de Doutoramento Sanduíche junto à Universidade de Lisboa – Portugal (2012). Mestre em Direito Constitucional pela UFSC (2005). Membro fundador e Presidente do Instituto Catarinense de Direito Público (ICDP). Membro fundador e Diretor Acadêmico do Instituto de Direito Administrativo de Santa Catarina (IDASC). Conselheiro Federal da OAB/SC. Presidente da Comissão Especial de Direito Administrativo da OAB Nacional. Coordenador do Grupo de Estudos em Direito Público do CCJ/UFSC (GEDIP/CCJ/UFSC). E-mail: jscristovam@gmail.com - <http://orcid.org/0000-0001-8232-9122>.

² Mestranda em Direito pelo PPGD/UFSC. Especialista em Direito Público (IMED) e Master Business Administration em Comércio e Relações Internacionais (UCS). Tem formação especializada em resolução pacífica de conflitos na Administração Pública Federal. Estudou na Università degli Studi di Roma, Itália e na Universidad Argentina de La Empresa. Integrante do Grupo de Estudos em Direito Público do CCJ/UFSC (GEDIP/CCJ/UFSC). Procuradora Federal. E-mail: hahn.tatiana@gmail.com - <https://orcid.org/0000-0001-6097-2491>.



1. Introdução

Em março de 2020, em Berlim, o Comitê Diretor da Parceria para o Governo Aberto (*Open Government Partnership - OGP*) (2020) aprovou o próximo plano de implementação, com duração de três anos e a nova direção estratégica para o Mecanismo de Relatório Independente da OGP. A organização expandiu e conta hoje com 78 membros nacionais, um número crescente de governos locais e milhares de participantes da sociedade civil foram criadas mais de 4000 reformas abertas do governo. Por outro lado, um contexto geopolítico mais amplo tem sido o retrocesso democrático, com o fechamento do espaço cívico e o aumento de políticas autoritárias e populistas, inclusive nos países membros do OGP.

Na medida em que o Brasil se aproxima, em 2012, do 10º aniversário do compromisso firmado por um governo aberto, é hora de avaliar o primeiro ciclo conectado por duas leis chaves no processo de abertura de dados, uma em cada extremidade: a Lei nº 12.527/2011 (Lei de Acesso à Informação – LAI) e a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados – LGPD). Além disso, cabe verificar o que foi construído dentro da Administração Pública e rever se as regras básicas do jogo são adequadas ao propósito do país para o futuro.³

A Controladoria-Geral da União (CGU) foi o órgão responsável por liderar a inserção do Brasil na OGP, articulando-se com diversos órgãos públicos e com setores da sociedade civil para construir o Plano de Ação Nacional, com o objetivo de difundir e incentivar internamente práticas governamentais relacionadas à transparência na gestão pública, ao acesso à informação, à participação social e ao início de uma formação de cultura de dados no país.

A par de outras normas brasileira, a LAI, após 8 anos de tramitação na Câmara dos Deputados, veio como fundamental passo na disciplina de acesso à informação, regulamentando o inciso XXXIII do art. 5º, o inciso II do § 3º do art. 37 e o § 2º do art. 216, da Constituição Federal. Na ponta contrária do acesso, como um dos frutos do progresso tecnológico mundial, a LGPD busca proteger dados pessoais e a privacidade do cidadão.

Não demorou para que a euforia causada pelo acesso a dados pela população e a ideia de abertura informacional pelo governo, estivesse marcada pela complexidade da gestão

³ O Brasil é membro fundador da OGP e assinou a Declaração de Governo Aberto em 20/09/2011, mesma data de aprovação do Decreto s/n (sem número), momento em que foi lançado o 1º Plano de Ação de Governo Aberto no país. Atualmente, o Brasil está no 4º Plano de Ação Brasileiro para Governo Aberto (BRASIL, 2020).



informacional nas sucessivas camadas administrativas de cada um dos três poderes e nos diversos níveis federativos. O trabalho seria longo. De fato, está sendo.

O esforço, por outro lado, é compensado pelo amadurecimento observado no Brasil e pelo reforço do sentimento de exercício de cidadania. Hoje temos discussões mais vivas e aprofundadas voltadas a entender o que são dados, à preocupação em protegê-los e à identificação de como a Administração Pública tem caminhado nesse tema.

A Administração Pública percorre quatro deveres de dados: o dever de abertura, o dever de transparência, o dever proteção e o dever de regulação, os quais podem ser na teórica objeto de estudos diferentes, mas, operacionalmente, devem ser analisados como um ciclo único e interligado.

No Brasil, projetos e iniciativas adotam o uso de dados como denominador comum para sua base de trabalho, seja por buscarem iniciativas de governo aberto e aprimoramento na transparência pública, seja por almejar o aumento de instrumentos de controle social, de programas de *compliance* público, de governança e transformação digitais.

No relatório da OCDE, publicado em novembro de 2019, a Organização defendeu a aproximação entre o governo e a população por meio do uso estratégico de dados, de modo que os Estados podem criar condições para: i) melhorar a qualidade de serviços públicos;⁴ ii) aumentar a eficácia de gastos públicos por meio de salvaguardas éticas; e, iii) desenvolver um manejo seguro e eficiente de dados. Tal processo visa tanto a conservação/criação de uma zona de confiança pública como também a entrega de resultados de gestão (OECD, 2019).

O relatório, ainda, sugere três áreas de discussão: i) a importância de um governo de dados; ii) o uso de dados para aumentar o valor público; e, iii) o papel dos dados na criação pública de confiança.

A questão é que, na prática, a base de dados já existe e foi formada antes da vigência de uma norma permissiva e na ausência de um planejamento estratégico. Os dados acumulam-se de modo progressivo e orgânico, em movimentos contínuos e dinâmicos por toda atividade administrativa, realidade que apresentou desafios e questões ao gestor no cotidiano administrativo. Por isso, são essenciais distinções quanto às espécies de dados envolvidos nas atividades da Administração Pública para a compressão sobre a gestão informacional, a execução de política de dados abertos e transparência ativa.

⁴ Sobre a questão da disrupção nos serviços públicos, inclusive com a proposta de superação do uso incremental das Tecnologias de Informação e Comunicação (TICs) no âmbito da Administração Pública 4.0, ver: CRISTÓVAM; SAIKALI; SOUSA, 2020.



Nesse texto, com base na Declaração de Governo Aberto da OGP e no relatório da OCDE, associados ao conceito de “valor público” de Mark Moore, objetiva-se, na primeira parte, tecer noções conceituais acerca dos tipos de dados que permeiam as funções administrativas e os respectivos dos fundamentos legais. Na segunda, trazer exemplos práticos de abertura de dados, bem como aspectos quanto à aplicação da INDA no Brasil.

2. Os dados e a Administração Pública brasileira

A Administração Pública como um todo, nas suas diversas esferas, é uma das maiores detentoras de dados no mundo. Dados esses em constante fluxo interno, de modo formal ou informal, em diferentes graus de organização, os quais costumavam ser recebidos, coletados, (re)processados e, por vezes, descartados, sem que se tivesse tamanha repercussão como se nota de uma década para cá.

Por noção de Administração Pública tem-se, aqui, aquela em sentido objetivo (CARVALHO FILHO, 2013, p. 11). Esta noção objetiva, prévia ao sentido subjetivo, está intrinsecamente conectada à preocupação e à aplicação do uso sustentável de dados, que são a impressão digital do que a sociedade pensa e age em um certo instante de tempo para saber como ela responderá no instante seguinte e assim por diante.

Mark Moore, em 1995, publicou um livro intitulado “*Creating Public Value*” (MOORE, 1995). A obra oferecia assessoria prática aos gestores públicos que buscavam fazer o melhor uso dos bens públicos que foram (temporariamente, com restrições e fiscalização significativas) confiados a eles. As ideias em torno de “valor público” foram desenvolvidas em um momento em que muitos conceitos de gestão ingressaram no setor público, o que levou, mais tarde, a uma promessa norte-americana por um setor público mais eficiente. Contudo, logo se observou que tais ideias levavam a desafios, pois os processos e práticas do governo democrático nem sempre se adaptavam particularmente bem aos paradigmas do setor privado. Além disso, permanecia uma incerteza sobre quem eram os clientes em questão, como eles poderiam estar melhor atendidos e quão isso era importante em comparação à uma missão geral (MOORE, 2013).

Tal concepção pública de gestão e de desempenho, baseada na preferência dos cidadãos, conduziu questionamentos e influenciou reformas nas teorias da *New Public*



*Management*⁵ e, a partir dos novos recursos oferecidos pela tecnologia da informação, levou Dunleavy a propor a teoria da *Digital-era Governance*.

Segundo Dunleavy (2014), a *New Public Management* (NPM) predominou no período entre 1980-2002, quando presenciamos a franca expansão da governança da era digital, a *Digital Era Governance* (DEG). Mesmo frente à pressão sobre os gastos públicos nas crises mundiais de crédito e financeira de 2008, Dunleavy identificou duas ondas de mudanças nos governos. A primeira onda na governança da era digital floresceu a importância dos principais temas do DEG reintegrando especificamente os serviços governamentais, promovendo uma entrega holística aos clientes e respondendo à onda de digitalização nos serviços públicos. Já a segunda, respondendo ao advento da web social, da computação em nuvem, do desenvolvimento de aplicativos e de outros fenômenos recentes, moveram as sociedades industriais avançadas ainda mais em direção à uma civilização *online*.

Ainda em 2013, Moore revisou sua própria obra e apresentou o estudo “*Recognizing Public Value*” fundada em uma visão de compromisso do setor público em desenvolver sistemas de medição de desempenho, não rasas e nem esporádicas (MOORE, 2013).

Nota-se que, embora Moore e Dunleavy analisassem modelos de gestão pública do século XXI e não propriamente a Administração Pública orientada por dados, eles apresentavam o fortalecimento da relação do Estado com o cidadão a partir do fluxo de informação entre eles. Desta forma, tanto a ideia de “valor público” quanto a de governo digital buscam, por meio de processos de tecnologia de informação, canalizar a atuação administrativa, fortalecer a confiança e entregar serviços com base em dados e no que eles comunicam à população.

Sabe-se que desde o século XVI há registro da coleta de informações sociais, mas é a partir do século XVII que, em função da necessidade de maior atuação do Estado nas áreas de defesa nacional e saúde, foi iniciado um movimento mais organizado de coleta de informações estatísticas em tópicos sociais. Nos séculos XVIII e XIX há uma intensificação dos movimentos de coletas e organização de dados nesse campo, o que introduziu o percurso para a construção dos modelos mais atuais de medição e coleta de características sociais (AMARAL, 2003, P. 9).

No Brasil, em 1871, ainda durante o período imperial, foi criado o primeiro órgão brasileiro para exercer atividades exclusivamente estatísticas, chamado de Diretoria Geral de

⁵ Sobre o tema, ver: TSUKUMO; PIMENTA; TERACINE, 2012.



Estatística (DGE), seguido do Decreto nº 5.604/1874 responsável pelo primeiro registro civil de forma formal e generalizada. Com o advento da República, foram ampliadas as atividades de apuração de dados, principalmente após a implantação do registro civil de nascimentos, casamentos e óbitos. Contudo, em 1934, o DGE agora já chamado de Departamento Nacional de Estatística foi extinto e as atribuições passaram aos ministérios competentes.

A carência de um órgão capacitado a articular e coordenar as pesquisas estatísticas, favoreceu a criação, no mesmo ano de 1934, do Instituto Nacional de Estatística (INE), cujas atividades iniciaram em 29 de maio de 1936. No ano seguinte, foi instituído o Conselho Brasileiro de Geografia, incorporado ao INE, que passou a se chamar, então, Instituto Brasileiro de Geografia e Estatística (IBGE), com a função de identificar e coletar dados sobre território, população, economia, trabalho, produção, política e modo de vida.

Antes disso, ainda durante o regime republicano, em especial a partir de 1927, foi desenvolvida no Brasil a Inteligência de Estado, chamada à época de Conselho de Defesa Nacional (CDN) e desde 1999 operada pela ABIN (Agência Brasileira de Inteligência) (Lei nº 9.883/1999), serviço que cruzou períodos democráticos e de exceção (durante as quatro fases de sua história), desenvolvendo atividades nos ramos de inteligência e de contrainteligência⁶ por meio do levantamento e do processamento de dados, em auxílio às decisões governamentais, na superação de obstáculos ou na análise de oportunidades. Já em junho de 1964, foi criado o Serviço Nacional de Informações (SNI) que trouxe à área de inteligência uma ampla estrutura nacional. O SNI foi instituído pela Lei nº 4.341, de 13/06/1964, com a função de “superintender e coordenar, em todo o território nacional, as atividades de informações e contrainformações, em particular as que interessem à Segurança Nacional”.

O compasso das estatísticas e dos dados foi evoluindo. Na década de 90, tornou-se uma das maiores tendências internacionais em Administração Pública um conjunto de ideias conhecidas como a Nova Administração Pública (NAP) (SEABRA, 2001), modelo que analisa a Administração Pública enquanto uma organização que recebe estímulo do ambiente

⁶ Para fins da Política Nacional de Inteligência (PNI), vigente hoje no Brasil, inteligência é atividade que objetiva produzir e difundir conhecimentos às autoridades competentes, relativos a fatos e situações que ocorram dentro e fora do território nacional, de imediata ou potencial influência sobre o processo decisório, a ação governamental e a salvaguarda da sociedade e do Estado. Já a contrainteligência objetiva a produção de conhecimentos e ações voltadas para a proteção de dados, conhecimentos, infraestruturas críticas (tais como comunicações, transportes, tecnologias de informação, ativos sensíveis e sigilosos de interesse do Estado e da sociedade). É a atividade que objetiva prevenir, detectar, obstruir e neutralizar a Inteligência adversa e as ações que constituam ameaça à salvaguarda de dados, conhecimentos, pessoas, áreas e instalações de interesse da sociedade e do Estado (BRASIL, ABIN, 2020).



(*input*), passam por um processo de transformação e transferem para o ambiente o resultado desse processo (*output*). Passamos das técnicas metodológicas de análise documental e de questionários impressos, para o *Big Data* e *Big Analytics*.

O movimento global em torno da disseminação de ferramentas de tecnologia da informação (TICs) e dos instrumentos digitais de conservação e armazenamento de dados com capacidade cada vez maiores, apresentou ao Estado uma nova perspectiva sobre o potencial gerencial, econômico e de direção das atividades públicas. Em verdade, observou-se também que dados podiam ser convertidos em informações úteis e não apenas enquanto dados isolados ou “crus” (*raw data*) (FRAZÃO, 2019, p. 26).

Essa nova perspectiva de relevância, segundo a qual quem detiver o maior volume de dados e informações terá o controle das circunstâncias em uma análise probabilística, igualmente revelou o quanto a Administração Pública deveria adotar medidas de segurança e proteção dos cidadãos e dos seus próprios agentes, sob a ótica da responsabilidade no tratamento das informações tuteladas por lei.

A mudança de paradigmas da organização e atuação administrativa públicas, em tempos em que os conceitos de *big data* são tão conhecidos, exige a clara compreensão sobre quais os tipos de dados são processados pelos seus agentes e colaboradores. Ou seja, a complexidade está em conhecer, classificar e aplicar o conjunto volumoso de informações geridas pelo Estado.

Dados, informações e conhecimento são conceitos diferentes. Dados são códigos, são a matéria prima, o estado bruto da informação, de tal forma que um conjunto de dados podem ou não representar algum conhecimento ou significado, podem ou não transmitir uma mensagem. Assim, em uma pesquisa eleitoral por exemplo, são coletados dados, isto é, mas somente se associados às perguntas que foram dirigidas, ao motivo e objetivo da pesquisa e integrada a soma de fatores demográficos e temporais é que teremos algo significativo. Daí a crescente preocupação em como manejar dados, pois é a partir deles que as informações e o conhecimento são (des)estruturados.

Os fatos e os dados, assim como as informações e o conhecimento, são vocábulos usualmente sobrepostos, mas que possuem natureza diversa na teoria da informação (RIBEIRO; SANTOS, 2020). Todavia, frente ao interesse jurídico, enfatizam a posição que os dados ocupam enquanto epicentro desse debate (DONEDA, 2006, p. 152).



Soma-se a isso o fato de que as tecnologias digitais mudaram a forma como as pessoas interagem, produzem e consomem produtos e serviços, o que demanda novas capacidades dos governos em responder a essa nova realidade social e em produzir processos e serviços mais inclusivos, transparentes (abertos). Mais que isso: gerir serviços e dados de modo a resguardar os direitos mais sensíveis, ponto crucial na conquista da confiança do cidadão e no ordenamento jurídico internacional.

A dizer: espera-se que a Administração Pública seja suficientemente aberta e transparente em seus dados, informações e conhecimento em prol do controle de sua eficiência e legalidade, mas não a ponto de extrapolar os limites da privacidade do cidadão ao expor dados pessoais de que tem acesso em razão da consecução de serviços públicos e análise de deveres civis. A balança entre esses dois vieses é sensível, dinâmica e complexa.

No Brasil, a combinação de fontes normativas permite distinguir os conceitos do que são dados abertos, dados anonimizados, dados pessoais, dados pessoais sensíveis, informações, informações classificadas e desclassificadas, o que por consequência permite ao intérprete identificar quais dados não estariam em nenhuma dessas categorias, que aqui denominaremos de “dados atípicos”.

Cabe atentar que o estudo dessas normas sofre implicações diante da forma fragmentada com que foram trazidas ao ordenamento, bem como de outras que ainda aguardam uma certeza jurídica quanto ao início de sua vigência, o que, em âmbito internacional, coloca o Brasil em uma posição anacrônica em relação aos demais países que trabalham com matrizes claras de como devem operar dados dentro da Administração Pública.

A proteção de dados ingressou no contexto constitucional brasileiro pela Constituição de 1988,⁷ como parte de um direito fundamental à inviolabilidade da comunicação de dados (art. 5º, XII), bem como recebeu instrumento constitucional próprio para assegurar seu titular o exercício de titularidade (art. 5º, LXXII) quanto ao conhecimento de seu conteúdo e a retificação em banco de dados.⁸

Quanto ao direito fundamental de inviolabilidade da comunicação telegráfica de dados, norma de eficácia contida, percebeu-se, nas decisões do Supremo Tribunal Federal

⁷ O Senado Federal, em sua biblioteca digital, tem o registro do primeiro habeas data concedido no Brasil em São Paulo noticiado em 12/10/1988 (BRASIL, Senado Federal, 1988).

⁸ A Lei nº 13.709/2018 conceitua, em seu art. 5º, inciso IV, banco de dados como o conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico (BRASIL, 2018).



(STF),⁹ uma clara cisão entre os termos “comunicação de dados” e “dos dados” propriamente ditos, como itens de tutela jurídica diversa a ponto de considerar objeto de proteção constitucional apenas “a comunicação telegráfica”, mas não seu produto, o qual seja o registro, os dados, deixando claro que estes não seriam objeto da proteção constitucional e, portanto, não seriam invioláveis os registros das comunicações telegráficas, tão-somente o momento em que a comunicação ocorria, em tempo real, mormente diante do parágrafo único do art. 1º da Lei nº 9.296/1996.¹⁰ Impossível não se questionar se essa visão fracionada persiste irretocável hoje, principalmente pois as formas de registros atuais são muito mais profundas e completas do que há uma década.

Curioso observar, contudo, que, embora a Constituição de 1988 não utilize a expressão “sigilo bancário”, a proteção constitucional aos dados deste sigilo foi conferida pela aplicação conjunta do mesmo inciso XII com o inciso X, ambos do art. 5º, situação em que se considerou que os dados bancários eram invioláveis por se referirem à intimidade, por serem dados pessoais que dependiam de proteção constitucional, ainda que não expressamente descrito.

Da mesma forma, o termo “dados” já era reconhecido como fonte para *accountability* fiscal e financeira quanto à arrecadação na forma do parágrafo único art. 162 constitucional, o que ganhou força em 27/05/2009, quando a Lei Complementar (LC) nº 131/2009, acrescentou dispositivos à LC nº 101/2000 (Lei de Responsabilidade Fiscal), a fim de determinar a disponibilização, em tempo real, de informações pormenorizadas sobre a execução orçamentária e financeira da União, dos Estados, do Distrito Federal e dos Municípios.

Sob o ponto de vista da gestão pública e transparência administrativa, a LC nº 101/2000, mormente após a LC nº 131/2009, ampliou a transparência sobre a gestão fiscal pública ao criar um canal de acesso à informação pública e de controle social para prover o

⁹ O STF, ao interpretar o art. 5º, XII, confirmou o entendimento de que “comunicação telefônica” e “registros telefônicos” recebiam proteção jurídica distinta, excluindo a interpretação da cláusula do artigo 5º, XII, da CF, quanto ao sentido de proteção aos dados enquanto registro, depósito registral e frisando que a proteção constitucional era da comunicação de dados e não dos dados. A título de exemplo: HC 91867, Relator Ministro Gilmar Mendes, Segunda Turma, julgado em 24/04/2012, publicado em 20/09/2012 (BRASIL, Supremo Tribunal Federal, 2012).

¹⁰ A Lei nº 9.296/1996, regulamentou o inciso XII, parte final, do art. 5º da CF e assim prevê: “Art. 1º. A interceptação de comunicações telefônicas, de qualquer natureza, para prova em investigação criminal e em instrução processual penal, observará o disposto nesta Lei e dependerá de ordem do juiz competente da ação principal, sob sigilo de justiça. Parágrafo único. O disposto nesta Lei aplica-se à interceptação do fluxo de comunicações em sistemas de informática e telemática” (BRASIL, 1996).



cidadão de dados públicos orçamentários¹¹ antes mesmo da edição Lei nº 12.527/2011, marco normativo da publicidade pública.

Nota-se, com esses breves apontamentos normativos, que a proteção de dados seguiu caminhos de resguardo constitucional segundo a função que exercem dentro da sociedade, bem como segundo o grau de vinculação com o titular e sua privacidade, mesmo quando não se tinha conhecimento claro do quanto que tais dados (públicos e privados) poderiam causar um dano caso a sua acessibilidade ou privacidade fossem quebrados hoje.

Do lado oposto ao sigilo, estão os “dados abertos” (dados comunitários). Segundo a *Open Knowledge Foundation (OKF)* (2019) “*dados são abertos quando qualquer pessoa pode livremente usá-los, reutilizá-los e redistribuí-los, estando sujeito a, no máximo, a exigência de creditar a sua autoria e compartilhar pelas mesmas regras*”. Por sua vez, quando os dados são produzidos, coletados ou custodiados por autoridades públicas e disponibilizados em formato aberto, considera-se que são dados abertos governamentais, tais como dados de cultura (dados sobre obras e artefatos culturais, coletados e mantidos por galerias, bibliotecas, arquivos e museus), dados de ciência (obtidos com como parte de pesquisas científicas da astronomia à zoologia), dados de finanças que já mencionamos (contas do governo com despesas e receitas, algumas informações sobre mercados financeiros como ações, ações, títulos), dados estatísticos (produzidos por órgãos públicos, como por exemplo o IBGE, como o censo e os principais indicadores socioeconômicos), dados climáticos (informações para prever o clima e eventos danosos e análise de mudanças climáticas) e dados ambientais (informações relacionadas ao meio ambiente natural, como presença e nível de poluentes, erosões, terrenos, qualidade e rios e mares).

A *OKF* também indica na avaliação do que seja um dado aberto as seguintes características: a) *disponibilização e acessibilidade*, tendo em vista que os dados devem estar disponíveis como um todo, com indicações de caminhos para facilitar o acesso e localização, evitando a exigência de registro das pessoas: isso restringe o número de respostas. e sob custo não maior que um custo razoável de reprodução (nem sempre serão gratuitos, mas que não valam para fins comerciais), preferencialmente possíveis de serem baixados pela internet por

¹¹ O Tribunal de Contas da União (TCU) entendeu que as informações sobre operações financeiras que envolvam recursos públicos não estão abrangidas pelo sigilo bancário a que alude a LC 105/2001, visto que operações da espécie estão submetidas aos princípios constitucionais da Administração Pública, de modo que é prerrogativa do TCU o acesso a essas informações, independentemente de autorização judicial. Acórdão 915/2017, Plenário, Relator Benjamin Zymler. Publicado Boletim de Jurisprudência nº 172 de 29/05/2017 (BRASIL, Tribunal de Contas da União, 2017).



qualquer pessoa; b) *reutilização e redistribuição*, de modo que os dados sejam fornecidos sob esses termos, inclusive a combinação com outros conjuntos de dados; c) *universalidade de gestão*, na medida em que estão habilitados a usar, reutilizar e redistribuir, sem distinção entre as áreas de atuação ou grupos pessoas. Assim, restrições de uso ‘não-comercial’ que impediriam o uso ‘comercial’, ou restrições de uso para certos fins (ex.: somente educativos) acabaria por excluir o enquadramento como dado aberto.

Internacionalmente, o grau de abertura de dados nos países é medido pelo *Open Data Barometer* (ODB) (2019), um projeto do *Open Data Institute* e da *World Wide Web Foundation* (responsável pela extensão www.w3.org) que buscam desenvolver métodos de avaliação para dados abertos. O projeto visa avaliar, por meio de pontuações, o impacto das iniciativas de dados abertos, analisar a disseminação da política governamental de dados abertos e como os países o colocam em prática em todo o mundo, inclusive com acolhimento de seus métodos, em 2014, o Tribunal de Contas da União (BRASIL, TCU, 2014).

Por outro lado, seriam exemplos de dados não abertos aqueles dados não atualizados, ou os não acessíveis pela internet ou, quando acessíveis *on-line*, necessitem de um *software* específico para acessá-los ou exigirem a identificação do interessado.

Registro relevante é que a LAI trata os “dados abertos” pela expressão “informações públicas”, assegurando tal acesso por meio da criação de um serviço público de informações responsável por receber, orientar e operar a tramitação desse procedimento em cada órgão sujeito ao normativo, na forma do art. 9º combinado com o art. 1º, ambos da LAI.

Um segundo conceito relevante à Administração Pública depois dos dados abertos, são os dados anonimizados. Consoante o art. 5º, inciso III da LGPD, é aquele dado relativo ao titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento. Desta forma, mesmo que o dado seja pessoal, para ser anonimizado é preciso que o usuário ou destinatário não tenha como associar a quem pertença a informação, direta ou indiretamente.¹² Desse modo, é a representação de dados sobre pessoa identificada, ou seja, é uma análise de potencial identificação que o torna pessoal, a chamada identificabilidade (MACHADO; DONEDA, 2018, p. 105).

¹² Segundo a LGPD, a Autoridade Nacional de Proteção de Dados (ANPD) poderá dispor sobre padrões e técnicas utilizados em processos de anonimização e realizar verificações acerca de sua segurança, ouvido o Conselho Nacional de Proteção de Dados Pessoais (BRASIL, 2018).



Desse modo, quando a Administração Pública executa funções por meio de servidores em trabalho remoto (seja em circunstâncias normais seja em excepcionais),¹³ um provedor de aplicação de internet, além de processar os dados de tráfego, armazenar registros de endereço IP de terminais que acessaram os sítios eletrônicos, permite que sejam facilmente identificados mediante requerimento judicial de acesso ou pelos termos de responsabilidade. Assim, esses registros de conexão e os dados cadastrais armazenados pelos respectivos provedores de conexão não são dados anonimizados, pois há a qualificação do endereço IP (dinâmico) como “informação relativa à pessoa natural identificada ou identificável”.¹⁴

Já dados pseudonimizados, segundo o art. 13, §4º, da LGPD, são aqueles, após tratamento, perdem a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro. Nesse sentido, a adoção desse tipo de procedimento (de anonimização ou pseudoanonimização dos dados) está tanto como uma medida de segurança (vinculado ao dever de repostar) como também para o caso de tratamento de dados pessoais que sejam usados fins de interesse público,¹⁵ investigação científica ou histórica, as quais devem ser estimuladas apenas se for possível preservar a segurança dos dados pessoais em seu manuseio (PINHEIRO, 2018).

Apresentados os campos de aplicação dos “dados abertos” e dos “dados anonimizados”, seguindo na linha principiológica de publicidade como preceito geral e sigilo como exceção, cumpre seguir para os conceitos de informação regulamentado pela LAI e que se aplica ao Poder Público.

Para efeitos da LAI considera-se “informação pessoal” aquela relacionada à pessoa natural identificada ou identificável (critério da identificabilidade) e o seu tratamento, previsto no art. 31 deverá ser feito de forma transparente, com respeito à intimidade, vida privada,

¹³ Exemplo recente de trabalho remoto em situação excepcional está na Instrução Normativa nº 19/2020 que estabelece orientações aos órgãos e entidades do Sistema de Pessoal Civil da Administração Pública Federal - SIPEC, quanto às medidas de proteção para enfrentamento da emergência de saúde pública de importância internacional decorrente da Covid-19 (BRASIL, 2020).

¹⁴ Entendimento adotado na União Europeia, tanto pelo Grupo de Trabalho de Proteção de Dados do Artigo 29, como pelo Tribunal de Justiça da União Europeia (TJUE) desde o julgamento do casos C-70/10, *Scarlet Extended SA v. Soci  t   belge des auteurs, compositeurs et   diteurs SCRL (SABAM)*, e C-582/14, *Patrick Breyer v. Bundesrepublik Deutschland*. Sobre o tema, ver: MACHADO; DONEDA, 2018, p. 107.

¹⁵ Ultrapassam os limites desse estudo o debate mais aprofundado sobre o conceito de interesse p  blico e sua centralidade para o regime jur  dico-administrativo. Apenas em breves considera  es, pode-se dizer que o “conceito de interesse p  blico confunde-se com os valores indispon  veis assegurados pela Constitui  o, sob o signo inafast  vel dos direitos fundamentais e da centralidade do princ  pio da dignidade da pessoa humana (personaliza  o da ordem constitucional)”. Sobre a no  o de interesse p  blico, ver: CRIST  VAM, 2015, p. 98-117.



honra e imagem das pessoas, bem como às liberdades e garantias individuais. Contudo, o Decreto nº 7.724/2012, regulamentador da LAI, traz conceito mais detalhado ao prever que informação pessoal é aquela relacionada à pessoa natural identificada ou identificável, relativa à intimidade, vida privada, honra e imagem, excetuando o consentimento do titular nas hipóteses dos art. 57 e 58.

Dessarte, a informação pessoal não goza de proteção temporária tal como a informação sigilosa, a qual fica submetida à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado ou em razão de hipóteses legais de sigilo. Nesse caso, cada órgão público deve conter o próprio rol de informações classificadas e desclassificadas, bem como os acréscimos respectivos da qualificação quanto ao grau de sigilo.

Segundo o art. 31 da LAI, as informações pessoais terão seu acesso restrito, independentemente de classificação de sigilo e pelo prazo máximo de 100 (cem) anos a contar da sua data de produção, mas poderão ter autorizada sua divulgação ou acesso por terceiros por previsão legal ou pelo consentimento expresso da pessoa titular das informações, sujeito o agente público ou militar à responsabilização conforme dispõem os artigos 32 a 34 do mesmo diploma.

Oportuno o registro de que as informações pessoais podem ser acessadas, sem consentimento ou previsão legal, quando necessárias à prevenção e diagnóstico médico, quando a pessoa estiver física ou legalmente incapaz, e para utilização única e exclusivamente para o tratamento médico, quando em atenção à ordem judicial ou à defesa de direitos humanos ou à proteção do interesse público e geral preponderante, conforme redação do art. 31, §3º, da LAI.

No que tange às informações públicas, importante mencionar a distinção entre as chamadas “informações classificadas” (reservadas, secretas e ultrassecretas, conforme estabelecido no art. 23 da LAI), e “desclassificadas”, tendo em vista que existem informações cuja divulgação indiscriminada expõe a risco a segurança da sociedade ou do Estado. Daí que, em que pese sejam dados públicos, a própria LAI restringe o acesso a esses dados por um tempo determinado, a depender do grau de sigilo. Isso demonstra que mesmo que uma informação ou dado sejam públicos, tal enquadramento não impede que haja uma restrição conforme classificadas em reservadas (prazo de cinco anos), secretas (prazo de quinze anos) e ultrassecretas (prazo de vinte e cinco anos), na forma do art. 23 da LAI, seguindo as



atribuições fixadas no art. 30, Decreto nº 7.724/2012 e formalizadas pelo Termo de Classificação de Informação (TCI).

Ainda na LAI, o art. 29 estabelece que os cidadãos podem solicitar a reavaliação da classificação das informações com vistas à sua desclassificação ou à redução do prazo de sigilo, bem como requerer a desclassificação, com rol que é anualmente divulgado pela autoridade máxima de cada órgão em cumprimento ao art. 30 da mesma lei, na forma prevista pelos artigos 45 e 73 do Decreto nº 7.724/2012.

Com efeito, enquanto uma antítese de dados anônimos, os dados pessoais representam a contemporaneidade que deverá passar a Administração Pública, daí seu relevo analítico. Além das duas referências legais quanto ao conceito de “informações pessoais” trazidas pela LAI e pelo Decreto nº 8.771/2016 e que deram suporte a um conceito expansionista de dados pessoais, com o alargamento da qualificação de dado como pessoal, agora a LGPD confirmou essa visão ao definir dado pessoal como a informação relacionada a pessoa natural identificada ou identificável no seu art. 5º, inciso I (BIONI, 2019, p. 68-70).

Por fim, embora o termo não seja próprio de normas jurídicas, mas frente à multidisciplinariedade da matéria de dados, oportuno o entendimento quanto ao conceito de “dados atípicos” como aquele conjunto de dados que pareçam inesperados pelo pesquisador, frente às suposições propostas em uma dada estatística ou que seja discordante ou contaminante. Assim, considerando que a Administração Pública aplica análise estatística de dados, os dados atípicos são aqueles que apresentam uma observação discordante (frente às suposições propostas em uma pesquisa), observação contaminante (que não venha da distribuição suposta no estudo), observação discrepante ou *outlier* (contaminante ao estudo). Esses dados são utilizados por pesquisadores com vários objetivos, dentre os quais a comparação de tratamentos, a verificação de certas suposições, ajuste de modelos ao conjunto de dados para evitar modelo inadequado, ou, simplesmente, a análise descritiva dos dados (MACHADO, 1997).

A partir da junção desses conceitos de dados custodiados pela Administração Pública é possível prosseguir no estudo empírico sobre a gestão informacional e governo aberto.

3. A abertura de dados, o Governo Aberto e a Infraestrutura Nacional de Dados Abertos (INDA)



Transmitir informações de forma confiável é chave para que os mal-entendidos não governem o mundo. No século XVII, momento que os governos já faziam as coletas de dados sociais como já referimos, Francis Bacon afirmava que não é tão fácil quanto podemos pensar transmitir um conceito da mente de um homem para a de outro sem uma perda, sem um erro, principalmente quando se tratam de noções novas e diferentes daquelas já estabelecidas ordinariamente (BACON, 2015). Os dados abertos se apresentam agora, na segunda década do século XXI, como ele condutor da comunicação pública entre o Estado e seus cidadãos e entre as nações.

Na década de 90, o termo “governo digital” foi oficialmente usado pela *National Performance Review*, nos Estados Unidos, quando o então Vice-Presidente, Albert Gore, apresentou linhas do plano do governo Clinton de reinventar do governo federal americano. Desde então os governos se empenham em fazer do governo digital um serviço voltado ao aumento da qualidade e da eficiência das operações internas de suas próprias atividades. Na medida em que a Administração Pública oferece serviços públicos usando canais eletrônicos em substituição progressiva dos demais canais tracionais, ganha-se envergadura às pautas de reforma administrativa e institucional no governo (GORE, 1993).

Ilustram essas inovações do Governo digital as consultas por parte dos cidadãos e ideação, contratações e coparticipação, e orçamento participativo, *crowdsourcing*,¹⁶ bem como a aplicação de inteligência artificial em serviços públicos nas mais diversas área e seguimentos,¹⁷ redes sociais de interação do Estado com o cidadão, aplicativos de serviços e, principalmente, o *Big Data*, este último um dos pontos de conexão com este trabalho.

Em setembro de 2011, o Brasil deu o primeiro passo à formação desse elo condutor pela Declaração de Governo Aberto ao assumir o compromisso de aumentar a disponibilidade das informações sobre as atividades governamentais e de interesse público. Aliada a esse ideal de governança, o direito administrativo contemporâneo precisa aplicar seus princípios a esse complexo processo de evolução de abertura de dados com objetivo de acolher a visão digital necessária à Administração Pública.

¹⁶ Da junção dos termos em inglês *crowd* (multidão) e *outsourcing* (terceirização) trata-se de um modelo multidisciplinar de produção e de estruturação de processos focados em aprendizados coletivos para a resolução de problemas e desenvolvimento de uma solução, ou seja, uma edificação coletiva e compartilhada. Por esse modelo, os dados abertos seriam fundamentais para coleta das informações envolvidas nesses processos a partir da definição de uma área a que se busque beneficiar. Daí que o termo é usualmente relacionado ao termo *crowdfunding* (financiamento coletivo).

¹⁷ Sobre a questão do uso das ferramentas de Inteligência Artificial (IA) aplicados pela Administração Pública federal nos seus sistemas de defesa no âmbito judicial, ver: CRISTÓVAM; HAHN, 2019.



Um dos maiores benefícios está em envolver os cidadãos nos processos de tomada de decisões e na formulação de políticas públicas voltadas aos objetivos fundamentais da República Federativa, notadamente quanto à construção de uma sociedade livre, em reduzir as desigualdades sociais e regionais e em ampliar das fontes envolvidas na elaboração dos programas de Estado desde os mais altos setores até os níveis locais e comunitários, em atenção ao art. 3º da Constituição de 1988.

Quando a Administração Pública está sob o encargo de aumentar o acesso à informação, seja por buscar alcançar os cidadãos ou facilitar a supervisão destes sobre as ações estatais, instrumentos e inovações típicas de um governo digital se misturam às maneiras anteriores de estudar o direito administrativo. Vale dizer: os gestores e operadores jurídicos se veem aglutinados à uma realidade prática e ao mesmo tempo imbuídos dos conhecimentos teóricos sobre regime jurídico administrativo que talvez não contassem com a mesma realidade.

Por isso, a receptividade dos ideais que a INDA e a respectiva gestão informacional que lhe é própria demandam dos gestores e operadores jurídico a visão de “um agir administrativo sob a perspectiva da consensualidade, da transparência, da construção de espaços abertos e democráticos de formação das decisões administrativas, do controle social e da eficiência da máquina pública” (CRISTÓVAM, 2014, p. 223).

Fato é que na medida em que se torna acessível ao público informações que, em verdade, sempre foram públicas, se permite empiricamente o controle social e a democratização da gestão informacional, peça decisiva na decisão administrativa e que habita – a quem se interessar, questionamentos do que ocorre na Administração Pública.

Por INDA se entende o conjunto de padrões, tecnologias, procedimentos e mecanismos de controle necessários para atender às condições de disseminação e compartilhamento de dados e informações públicas no modelo de Dados Abertos, em conformidade com os Padrões de Interoperabilidade de Governo Eletrônico (e-PING).¹⁸ Desta forma, a INDA objetiva ser o ponto referencial para o compartilhamento e uso de dados públicos (abertos) com vistas ao incentivo da oferta desse tipo de dado, bem como para uma formação padronizada e centralizada em catálogo governamental.

¹⁸ A arquitetura ePING define um conjunto mínimo de premissas, políticas e especificações técnicas que regulamentam a utilização da TIC na interoperabilidade de serviços de Governo Eletrônico, estabelecendo as condições de interação com os demais Poderes e esferas de governo e com a sociedade em geral (BRASIL, 2019).



Nessa linha, uma infraestrutura de dados abertos permite que haja um trabalho em prol de um governo aberto, de um governo digital, expressões complementares e não sinônimas. Consequentemente, o INDA propõe quatro princípios centrais à ideia de governo aberto: i) transparência: os dados sobre as atividades governamentais são abertas, compreensíveis, tempestivas, livremente acessíveis e atendem ao padrão básico de dados abertos;¹⁹ ii) *accountability*: atuação por regras e mecanismos que estabelecem e justificam ações, bem como sobre críticas e exigências de modo a aceitar as responsabilidades que lhes são incumbidas; iii) participação cidadã: adoção de mecanismos que mobilizem a sociedade em debater, em colaboração e na proposta de contribuições efetivas a um governo mais eficaz e responsivo e; iv) tecnologia e inovação: reconhecimento de novas tecnologias e no fomento à inovação como chave essencial nesse processo.

Nota-se que as ações estatais serão consideradas próprias de um governo aberto enquanto (e se) sua gestão, ações, projetos e programas refletirem dinamicamente a soma desses quatro princípios e que podem ser representados respectivamente por quatro objetivos da Declaração de Governo Aberto da OGP: a) aumento da disponibilidade de informações sobre atividades governamentais; b) implemento de padrões mais altos de integridade profissional na Administração; c) apoio à participação social e; d) ampliação do acesso a novas tecnologias para fins de abertura e prestação de contas.

A INDA²⁰ é, ainda, o meio pelo qual será gerida a Política de Dados Abertos (art. 5^a, do Decreto nº 8.777/2016) e que deve atender o princípio da legalidade, a agenda internacional direcionados à promoção da transparência e da participação social na gestão pública.²¹

¹⁹ O art. 8º, da LAI estabelece que as informações de interesse coletivo ou geral devem ser obrigatoriamente divulgadas pelos órgãos e entidades públicos em seus sítios oficiais, os quais devem atender, entre outros, aos seguintes requisitos: i) possibilitar o acesso automatizado por sistemas externos em formatos abertos; ii) serem estruturados e legíveis por máquina; iii) estarem acompanhados de detalhes sobre os formatos utilizados para estruturação da informação; iv) serem autênticos, íntegros e atualizados. Nesse sentido, remetemos o leitor ao tópico sobre transparência e ao conceito de transparência ativa (BRASIL, 2012).

²⁰ Atentamos ao leitor que, atualmente, está em processo de formação na CGU a minuta de Portaria para reestruturação da INDA. A minuta está disponível em: <https://www.gov.br/cgu/pt-br/assuntos/noticias/2020/05/aberta-consulta-publica-sobre-reestruturacao-da-infraestrutura-nacional-de-dados-abertos>. Acesso em: 17 jul. 2020.

²¹ A Instrução Normativa SLTI/MP nº 4/2012 instituiu a INDA. Ainda, nesse rol caberia a inclusão do Decreto nº 8.243/2014 que institui a Política Nacional de Participação Social - PNPS e o Sistema Nacional de Participação Social - SNPS. O PNPS tinha como objetivo fortalecer e articular os mecanismos e as instâncias democráticas de diálogo e a atuação conjunta entre a Administração Pública Federal e a sociedade civil. Contudo, esse decreto foi integralmente revogado pelo Decreto nº 9.759/2019 que extingue e estabelece diretrizes, regras e limitações para colegiados da administração pública federal. O referido decreto já foi parcialmente alterado pelo Decreto nº 9.812/2019. Além disso, cabe referir que tramita no Supremo Tribunal



Sob o aspecto de auditoria, em 2014, o TCU, por intermédio da Secretaria de Fiscalização de Tecnologia da Informação (SEFTI), realizou levantamento com o objetivo de conhecer iniciativas de publicação de dados abertos na Administração Pública Federal e em âmbito internacional, resultando no Acórdão Plenário nº 2.569/2014,²² quando se recomendou à SEFTI que examinasse a viabilidade da inclusão, em futuros planos de fiscalização, da realização de ações de controle voltadas à verificação da implementação da política de abertura de dados nas unidades da Administração Pública Federal, bem como da realização de ações de estímulo à conscientização dessas unidades acerca de conceitos, objetivos, legislação, indicadores, riscos e estruturas de governança relacionados ao tema dados.

Seguindo nesse contexto de infraestrutura normativa sobre dados abertos, importa destacar a importância do Decreto nº 8.777/2016 que instituiu a Política de Dados Abertos (PDA) do Poder Executivo Federal, inclusive de forma a incentivar iniciativas municipais e estaduais em todo o país e que teve significativas alterações pelo Decreto nº 9.903/2019.

Também em 2016, a publicação do Decreto nº 8.638 apresentou a Política de Governança Digital no âmbito dos órgãos e das entidades da Administração Pública federal direta, autárquica e fundacional, hoje sob o regulamento do Decreto nº 10.332/2020, que definiu a Estratégia de Governo Digital para o período de 2020 a 2022 com inclusão do Plano de Dados abertos como um instrumento de planejamento dessa estratégia, no art. 3º, inciso III.

Já o Decreto nº 9.319/2018 foi responsável por instituir o Sistema Nacional para a Transformação Digital (SinDigital),²³ bem como por estabelecer a estrutura de governança

Federal (STF), a ADI 6121, com decisão final pendente, mas com medida cautelar liminar parcialmente deferida com a seguinte ementa: PROCESSO OBJETIVO. CONTROLE DE CONSTITUCIONALIDADE. LIMINAR. DEFERIMENTO PARCIAL. Surgindo a plausibilidade jurídica parcial da pretensão e o risco de manter-se com plena eficácia o quadro normativo atacado, impõe-se o deferimento de medida acauteladora, suspendendo-o. COMPETÊNCIA NORMATIVA. ADMINISTRAÇÃO PÚBLICA. ÓRGÃOS COLEGIADOS. PREVISÃO. LEGAL. EXTINÇÃO. CHANCELA PARLAMENTAR. Considerado o princípio da separação dos poderes, conflita com a Constituição Federal a extinção, por ato unilateralmente editado pelo Chefe do Executivo, de órgãos colegiados que, contando com menção em lei em sentido formal, viabilizem a participação popular na condução das políticas públicas – mesmo quando ausente expressa “indicação de suas competências ou dos membros que o compõem” (ADI 6121 MC, Relator Min. Marco Aurélio, Tribunal Pleno, julgado em 13/06/2019, publicado em 28/11/2019) (BRASIL, Supremo Tribunal Federal, 2019).

²² O acórdão resultou do processo nº 005.003/2014-8, autuado em 10/03/2014, por um relatório de levantamento, com o seguinte assunto: “conhecer as iniciativas de dados abertos na APF (administração pública federal), considerando ainda o uso atual de soluções de coleta, armazenamento e processamento de grandes volumes de dados (Big Data) pelo governo e sociedade como estratégias de transparência e modernização da gestão pública (BRASIL, Tribunal de Contas da União, 2014).

²³ O mesmo decreto criou a Estratégia Brasileira para a Transformação Digital - E-Digital com vistas à harmonização das iniciativas do Poder Executivo Federal ligadas ao ambiente digital, ao aproveitamento do potencial das tecnologias digitais. Visa também por essa estratégia promover o desenvolvimento econômico,



para a implantação da Estratégia Brasileira para a Transformação Digital, diretamente vinculada à PDA como parte dessa visão estratégica. Ainda, o Decreto nº 10.046/2019 dispõe sobre a governança no compartilhamento de dados, seus níveis e categorização dos dados para o compartilhamento entre os órgãos no âmbito da Administração Pública federal (em todos seus poderes), além de regular o Cadastro Base do Cidadão²⁴ e o Comitê Central de Governança de Dados.²⁵

Cabe destacar que a LAI aperfeiçoou a ideia de transparência ao dispor que as informações de interesse coletivo ou geral produzidas por órgãos e entidades públicas devem ser obrigatoriamente divulgadas em sítios oficiais na internet, que deverão possibilitar a gravação de relatórios em diversos formatos eletrônicos, inclusive abertos e não proprietários. Nesse sentido, a abertura de dados governamentais não se apresenta como mera alternativa de viabilização da transparência pública, mas como um dever a ser cumprido pelo administrador público.

Internacionalmente, a OCDE indica os seguintes benefícios para um governo de abertura de dados: a) responsabilização e prestação de contas (*accountability*), uma vez ser necessário a existência de mecanismos que possibilitem aos cidadãos fiscalizarem o governo quanto ao desempenho de suas políticas e de seus serviços; b) transparência, pois a disponibilização de informações confiáveis, relevantes e tempestivas sobre as atividades do Estado permite que os cidadãos compreendam as ações públicas; c) participação social, tendo em vista que o governo deve escutar os cidadãos e considerá-los os seus anseios, tanto no desenho quanto na implementação das políticas públicas e dos serviços públicos prestados (OECD, 2019).

Considerando esse conjunto normativo brasileiro sobre a infraestrutura nacional de dados, é oportuno sublinhar alguns exemplos positivos no uso de dados abertos como

social sustentável e inclusivo, com inovação, aumento de competitividade, de produtividade e dos níveis de emprego e renda no País, na forma do seu art. 1º, §1º (BRASIL, 2018).

²⁴ Criado pelo decreto em outubro de 2019, o Cadastro Base do Cidadão é uma iniciativa que busca desburocratização do governo digital. O acesso ao Cadastro Base do Cidadão se dará por meio de duas soluções tecnológicas disponibilizadas pela Receita Federal: a *blockchain* bCPF e a *API Light*, por meio das empresas públicas de tecnologia da informação (TI) Dataprev e Serpro, respectivamente. Os dados a serem compartilhados pela bCPF ou pela *API Light* são os dados cadastrais da Base da Receita (não abrangidos pelo sigilo fiscal e enumerados art. 18 do Decreto nº 10.046/2019). Em 2017, o Brasil passou a identificar o brasileiro em suas relações com a sociedade e com os órgãos e entidades governamentais e privados por meio da Identificação Civil Nacional (ICN), criada pela Lei nº 13.444/2017 (BRASIL, 2019).

²⁵ O referido comitê é regido pela Resolução ME nº 1/2020 e já publicou a versão 1.0 sobre regras para o compartilhamento de dados entre os órgãos e as entidades da administração pública federal direta e autárquica e fundacional e os demais Poderes da União, excluídos os conselhos de fiscalização profissionais (BRASIL, 2020).



instrumentos ativos de controle e de inclusão digitais, com vistas à transparência e à eficiência na atividade administrativa.

Com reconhecimento de modelo nacional, em trabalho na linha do modelo da *OKF*, seguindo o modelo federal, o Município de Recife (Pernambuco) desenvolveu um portal no qual concentra dez pastas administrativas, organiza nove temas de interesse público com uso de cinquenta etiquetas (além das subetiquetas), com mais de seis formatos para extração dos dados, licenciados e uma descrição completa de fontes e mapas de calor.

O Município de São Paulo, por sua vez, via Secretaria Municipal de Inovação e Tecnologia, ampliou as políticas de dados abertos e transparência, por intermédio do lançamento da Vitrine de APIS da Cidade de São Paulo – a APILIB, medida irá permitir a conexão de sistemas ou aplicações das bases públicas de dados, bem como fomentar a criação de serviços e aplicações que gerem valor público, com associação inicial de bases de dados sobre compras e licitações, dados de ligações e reclamações dos canais, índice de desenvolvimento humano municipal, reclamações e denúncias (PROCON Paulistano), pedidos de informação protocolados na via e-SIC, base de dados sobre lentidão por trechos e Escola Aberta, entre outros (SÃO PAULO, 2020).

Na mesma esteira, com uma base de mais de 10 milhões de registros na área de educação, de atualização mensal e anual, o Estado de Santa Catarina (SC) concentrou os dados da rede de ensino no suporte à gestão e à tomada de decisões com análise em matrículas, unidades de ensino, distorção idade-série, infrequência e desempenho escolar, bem como no intuito de acompanhar a posição das escolas catarinenses em pesquisas e relatórios nacionais (SANTA CATARINA, 2020).

O plano é buscar uma análise preditiva com respostas rápidas às fragilidades existentes para balizar ações pela melhoria na qualidade da educação. Entre outros exemplos em áreas como segurança, interessante medida na área econômica, os principais indicadores econômicos catarinenses estão disponíveis mensalmente em um Boletim de Indicadores Econômico-Fiscais com estatísticas econômicas oficiais, abrangendo informações sobre balança comercial, produção agrícola e industrial, volume de vendas e receitas do comércio, número de empresas constituídas e baixadas, consumo de energia elétrica (SANTA CATARINA, 2019).

Referência em dados financeiros, o “Orçamento ao seu Alcance”, portal desenvolvido pelo INESC (Instituto de Estudos Socioeconômicos), em parceria com a *OKF*



Brasil, ampliou-se a consulta ao orçamento federal pelo acompanhamento do desembolso financeiro dos Ministérios e demais órgãos federais. O sistema coleta dados do SIGA Brasil mantido pelo Senado Federal, o qual permite acesso amplo aos dados do Sistema Integrado de Administração Financeira (SIAFI) e outras bases de dados sobre planos e orçamentos públicos (INESC, 2019).

Nota-se que a abordagem prática dos dados abertos é primordial ao gestor público, notadamente frente à visão de interoperabilidade²⁶ na Administração Pública (CORRÊA, 2012), linguagem da gestão informacional²⁷ e que trabalha com a capacidade de diversos sistemas e organizações interoperarem, se comunicarem de forma transparente e/ou com combinarem diferentes conjuntos de dados que historicamente estão em processo de coleta (SILVA, 2004).

Para ilustrar como ocorre e importância da interoperabilidade na Administração Pública, trazemos o exemplo dos serviços da Imprensa Nacional, responsável pela publicação de matérias, de todas as ordens e de todos os poderes, no Diário Oficial da União (DOU). Assim, quando o sistema de Gestão Eletrônica de Documentos (GED) de um órgão criar a nomeação de um servidor e enviar para a Imprensa Nacional, há a devolução da informação sobre o dia em que vai ser publicada a nomeação, quanto custará e uma pré-visualização do resultado, o que permite que o servidor inicie e finalize seu trabalho sem a necessidade de acessar vários sistemas de órgãos diferentes, com a disponibilidade da informação na tela de seu sistema. Outro exemplo são os certificados digitais emitidos²⁸ na cadeia de confiança ICP-

²⁶ A interoperabilidade entre aplicações e base de dados está prevista entre os objetivos de promoção da Lei nº 12.965/2016 (Marco Civil da Internet) e como uma das diretrizes da atuação do poder pública na internet, segundo os artigos 4º e 24, de modo que o governo federal possui uma plataforma de Interoperabilidade, Infraestrutura Tecnológica que propicia, como descrito no texto, a integração entre os serviços públicos, compartilhamento de informações governança dos ativos e processos de integração (BRASIL, 2016)

²⁷ Os conceitos de interoperabilidade e integração, em que pesa possam ser utilizados como sinônimos na área de TICs, são conceitos distintos e complementares, de modo que a escolha pela interoperabilidade está pela realização do processo de comunicação, enquanto a integração está mais na conexão, ou seja, é um facilitador. Interesse exemplo de integração ocorreu no Ministério da Saúde, onde cada sistema possuía seu próprio cadastro de hospitais e postos de saúde, sem que fosse possível cruzar esses dados ou mesmo listar as atividades de cada instituição. Logo, as instituições também precisavam manter atualizados vários cadastros dentro do MS. A solução foi a criação de um cadastro central, o Cadastro Nacional de Estabelecimentos em Saúde (CNES), que integra todas as bases de hospitais e postos de saúde e permitiu (por integração) que o Ministério da Saúde tivesse um mapa claro das instituições em saúde no Brasil, inclusive com atualização constante direta no mesmo sistema.

²⁸ O certificado Digital é o documento eletrônico que possibilita a troca segura de informações entre duas partes, com a garantia da identidade do emissor. A primeira autoridade certificadora credenciada pela Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), foi o Serpro que desde a criação do Centro de Certificação Digital Serpro, em 1999, viabiliza o uso dessa tecnologia por cidadãos, governo, empresas e poder judiciário (BRASIL, SERPRO, 2020).



Brasil que obedecem a padrões técnicos o que possibilita – independente da Autoridade Certificadora que emitiu o Certificado Digital – a interoperabilidades com as aplicações existentes, cada vez com soluções avançadas de *blockchain* principalmente para o sistema financeiro, com maior eficiência e confiabilidade.

4. Considerações finais

A avaliação dos limites do fluxo informacional dentro da Administração Pública exige a distinção clara quanto às espécies dos dados em jogo, bem como o balanceamento constante entre os benefícios e obrigações decorrentes do dever de transparência pública.

Nesse processo se destacou a confiança enquanto elemento mais sensível no progresso e manutenção de abertura de dados e se mostra ainda mais desafiadora para restaurar caso seus instrumentos sejam falhos, insuficientes ou não visem o dever de integridade e o alcance daquilo que de fato possui “valor público” à população.

A Administração Pública orientada por dados precisa explorar as determinantes dessa confiança (proteção de dados pessoais, confiabilidade, justiça, integridade, capacidade de resposta e abertura) e compreender, por meio dos seus gestores e servidores, como apresentar boas práticas sobre o uso de dados. Além disso, em um ambiente plural, pleno de informações, e com regras de participação conhecidas, é possível gerar um padrão de atratividade à cidadania que hoje, em muitos campos, ainda não se logrou alcançar (VALLE, 2011, p. 152).

Organizar as ideias envolvidas nas ações públicas relacionadas a dados no Brasil é como construir uma casa, em que cada pedaço solidificado permite a maior proteção de quem (do que) estiver sob seu teto. Expandir as ideais sociais de liberdade de informação, de um Governo Aberto, é também atribuir uma responsabilidade aos cidadãos para que assumam papel de agente de transformação social (não de meros telespectadores e replicantes). Afinal, não esqueçamos que o impulso e a euforia por essa clareza de dados também carregam a mudança dos sapatos que calçamos, de modo que cada um de nós será (já é) participante do teor dessas informações e poderá (deverá) se questionar como contribuir responsivamente a elas.

Referências

AMARAL, Roberto Montello. *A avaliação de resultados no setor público: teoria e aplicação prática no Estado do Rio de Janeiro*. Rio de Janeiro: Tribunal de Contas do Estado do Rio de



Janeiro, 2003. Disponível em:

http://antigo.enap.gov.br/downloads/ec43ea4faval_resul_no_setor_pub.pdf. Acesso em: 2 mai. 2020.

BACON, Francis. *Valerius Terminus: Of the Interpretation of Nature. Wealth Of Nation*. Edição do Kindle. Ebook, 2015.

BIONI, Bruno. *Proteção de dados pessoais: a função e os limites do consentimento*. São Paulo: Forense, 2019.

CARVALHO FILHO, José dos Santos. *Manual de direito administrativo*. 26. ed. São Paulo: Atlas, 2013.

CORRÊA, Andreiuid Sheffer. *Metodologia para aferição do nível de maturidade associado à interoperabilidade técnica nas ações de governo eletrônico*. 128 f. Dissertação de Mestrado Profissional da Pós-Graduação do Centro de Ciências Exatas da PUC-Campinas, Campinas, 2012. Disponível em: <http://tede.bibliotecadigital.puc-campinas.edu.br:8080/jspui/handle/tede/525>. Acesso em: 2 mai. 2020.

CRISTÓVAM, José Sérgio da Silva. *Administração Pública democrática e supremacia do interesse público: novo regime jurídico-administrativo e seus princípios constitucionais estruturantes*. Curitiba: Juruá, 2015.

CRISTÓVAM, José Sérgio da Silva. O direito administrativo no divã do Estado constitucional de direito: a travessia da legalidade para a juridicidade administrativa. *Revista da ESMESC*, Florianópolis, v. 21, n. 27, p. 195-228, 2014.

CRISTÓVAM, José Sérgio da Silva; SAIKALI, Lucas Bossoni; SOUSA, Thanderson Pereira de. Governo Digital na Implementação de Serviços Públicos para a Concretização de Direitos Sociais no Brasil. *Seqüência: Estudos Jurídicos e Políticos*, Florianópolis, v. 43, n. 84, p. 209-242, abr. 2020. Disponível em: <https://periodicos.ufsc.br/index.php/sequencia/article/view/2177-7055.2020v43n84p209/43642>. Acesso em: 2 mai. 2020.

CRISTÓVAM, José Sérgio da Silva; HAHN, Tatiana Meinhart. Instrumentos de automação da defesa judicial aplicados pela administração pública federal brasileira: do eletrônico ao digital. *Revista Democracia Digital e Governo Eletrônico*, Florianópolis, v. 1, n. 18, p. 127-143, 2019. Disponível em: <http://buscalegis.ufsc.br/revistas/index.php/observatoriodoegov/article/view/317>. Acesso em: 2 mai. 2020.

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

DUNLEAVY, Patrick; MARGETTS, Helen Zerlina. The Second Wave of Digital Era Governance. APSA, 2010, *Annual Meeting Paper*, 2014. Disponível em: <https://ssrn.com/abstract=1643850>. Acesso em: 2 mai. 2020.

FRAZÃO, Ana. Fundamentos da proteção dos dados pessoais. In: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (Coord). *Lei Geral de Proteção de Dados e suas repercussões no direito brasileiro*. São Paulo: Revista dos Tribunais, 2019.

GORE, Albert. *From red tape to results: Creating a government that works better and costs less*. Report of the national performance review. Diane Publishing, 1993. E-book.



MACHADO, Diego; DONEDA, Danilo. Proteção de dados pessoais e criptografia: tecnologias criptográficas entre anonimização e pseudonimização de dados. *Revista dos Tribunais – Caderno Especial*, São Paulo, v. 998, p. 99-128, 2018.

MOORE, Mark H. *Creating Public Value: strategic management in Government*. London: Harvard University Press. 1995.

MOORE, Mark H. *Recognizing Public Value*. Harvard University Press. Edição do Kindle, 2013. E-book.

OECD. The Path to Becoming a Data-Driven Public Sector, *OECD Digital Government Studies*, OECD Publishing, Paris, 2019. Disponível em: <https://doi.org/10.1787/059814a7-en>. Acesso em: 2 mai. 2020.

RIBEIRO, Nivaldo Calixto; SANTOS, Sarah Rúbia de Oliveira. Desenho da informação na perspectiva da ciência da informação. *LOGEION: Filosofia da Informação*, Rio de Janeiro, v. 6, n. 2, p. 132-141, mar./ago. 2020. Disponível em: <http://revista.ibict.br/fiinf/article/view/5124/4550>. Acesso em: 2 mai. 2020.

SEABRA, Sérgio Nogueira. A nova Administração Pública e mudanças organizacionais. *Revista de Administração Pública*, Rio de Janeiro, v. 35, n. 4, p. 19-43, 2001. Disponível em: <http://bibliotecadigital.fgv.br/ojs/index.php/rap/article/view/6394/4979>. Acesso em: 2 mai. 2020.

SILVA, Rafael Ferreira. *A importância da interoperabilidade*. ago. 2004. Disponível em: <http://phpbrasil.com/articles/article.php/id/851>. Acesso em: 2 mai. 2020.

TSUKUMO, Alfredo Nozomu; PIMENTA, Márcia de Fátima; TERACINE, Edson. A Tecnologia da Informação propiciando novos rumos para a Administração Pública. *Publicações da Escola da AGU*, Brasília, n. 23, 2012.

VALLE, Vanice Regina Lírio do. *Direito fundamental à boa administração e governança*. Belo Horizonte: Fórum, 2011.