

Manifestação Técnica

PG/PADM/T/025/2021/AFC

Em 12 de abril de 2021

REFERÊNCIA: PROCESSO N. 04/000.287/2021

DIREITO CONSTITUCIONAL E TRIBUTÁRIO. SIGILO FISCAL DE DADOS. TRIBUNAL DE CONTAS DO MUNICÍPIO. REQUERIMENTO DE ACESSO A BANCO DE DADOS PESSOAIS DE NATUREZA FISCAL. SISTEMA DE INTELIGÊNCIA FISCAL – SIF. INFORMAÇÕES SIGILOSAS, SUSCETÍVEIS DE IDENTIFICAÇÃO E DE QUANTITATIVO INDETERMINÁVEL DE PESSOAS. DIREITO FUNDAMENTAL À AUTODETERMINAÇÃO INFORMACIONAL NA CONSTITUIÇÃO BRASILEIRA: DE DIREITO IMPLÍCITO A DIREITO AUTÔNOMO CONSAGRADO PELO SUPREMO TRIBUNAL FEDERAL. LEI GERAL DE PROTEÇÃO DE DADOS: CONSIDERAÇÕES GENÉRICAS, DIANTE DE SUA TRANSVERSALIDADE A OUTROS TEMAS DA ADMINISTRAÇÃO PÚBLICA MUNICIPAL, E ANÁLISE DA INCIDÊNCIA IN CONCRETO. MUNICÍPIO DO RIO DE JANEIRO COMO ENTE CONTROLADOR. RESPONSABILIDADE. NECESSIDADE DE FORMULAÇÃO DE CONVÊNIOS E INSTRUMENTOS CONGÊNERES PARA COMPARTILHAMENTO DE DADOS ENTRE ÓRGÃOS E ENTIDADES DO PODER PÚBLICO. FINALIDADE ESPECÍFICA. ESPÉCIES DE INFORMAÇÕES DISPONÍVEIS NÃO DELIMITADAS, NÃO CORRELACIONADAS A PROCESSO ADMINISTRATIVO ESPECÍFICO E CUJA MOTIVAÇÃO SERIA O EXERCÍCIO DO CONTROLE EXTERNO PER SE. AUSÊNCIA DE EXIGÊNCIAS NORMATIVAS E PRINCIPIOLÓGICAS DA LEI GERAL DE PROTEÇÃO DE DADOS, DE PREVISÃO LEGAL, BEM COMO DOS REQUISITOS IMPOSTOS PELA JURISPRUDÊNCIA DO SUPREMO TRIBUNAL FEDERAL EM MATÉRIA DE SIGILO DE DADOS FISCAIS EM ESPECÍFICO. IMPOSSIBILIDADE A PRIORI.

I – RELATÓRIO

Trata-se de consulta realizada pelo Subsecretário de Tributação e Fiscalização em virtude de requerimento formulado pelo Tribunal de Contas do Município do Rio de Janeiro, para que a Secretaria Municipal de Fazenda e Planejamento disponibilize, para os auditores daquele órgão, **acesso integral ao Sistema de Inteligência Fiscal – SIF.**

Conforme relatório do Subsecretário, o citado **sistema conjuga diversas bases de dados de diversos sistemas tributários da Prefeitura da Cidade do Rio de Janeiro** e de outras fontes, através de convênios em que a confidencialidade é garantida. Sendo assim, a dúvida da Pasta é em relação à violação ao **sigilo fiscal**, haja vista o disposto no art. 198 do Código Tributário Nacional.

É o relatório.

II – ANÁLISE JURÍDICA

A matéria em exame envolve o tema do sigilo fiscal, a saber, do resguardo dos dados fiscais dos contribuintes que ficam sob custódia da Fazenda Pública diante de sua prerrogativa de cobrar tributos para fazer frente ao pagamento das despesas públicas, de modo que o sigilo fiscal de dados pessoais não deixa de ser uma especificação de um *direito à autodeterminação informacional* consagrado constitucionalmente e que merece tratamento preliminar e genérico, na medida em que poderá servir de parâmetro, por sua transversalidade, a uma série significativa de outras situações jurídicas nas quais compete ao Poder Público protegê-la, inclusive, dele mesmo.

Por tais razões, esta manifestação técnica será dividida em três Partes, cujo sumário, mais adiante, se apresenta: um *primeiro*, em que se trata do direito à *autodeterminação informativa*, seja como direito autônomo, para uns, seja como expressão da personalidade e garantia da privacidade, da imagem e da individualidade, para outros; um *segundo*, em que se destrincha a aplicação da Lei Geral de Proteção de Dados no âmbito da Administração Pública em geral, apontando sua incidência ao caso concreto, no que

couber; e, finalmente, um *terceiro*, em que se analisa minudentemente a proteção de dados sob a ótica do sigilo fiscal.

Nesta linha de ideias, tem-se o seguinte:

SUMÁRIO

PARTE I – DIREITO FUNDAMENTAL À AUTODETERMINAÇÃO INFORMACIONAL
PARTE II - FUNDAMENTOS JURÍDICOS EM MATÉRIA DE PROTEÇÃO DE DADOS PESSOAIS NA LEI GERAL DE PROTEÇÃO DE DADOS
PARTE III - FUNDAMENTOS JURÍDICOS EM MATÉRIA DE PROTEÇÃO DE DADOS PESSOAIS COBERTOS POR SIGILO FISCAL

PARTE I – DIREITO FUNDAMENTAL À AUTODETERMINAÇÃO INFORMACIONAL

“O homem de lata que anseia um coração deixou as longínquas narrativas de O Mágico de Oz (1939) e passou a ocupar a realidade contemporânea por meio da Internet das Coisas (Internet of Things ou IoT): robôs que têm sentimentos, máquinas que pensam e aprendem sozinhas, TVs que captam as emoções de seus telespectadores e, assim, podem recomendar-lhes filmes. Em um contexto de tão frequente inovação, a ficção torna-se realidade, a multidão torna-se nua e a proteção de dados pessoais assume caráter indispensável ao progresso democrático e social.”¹

Segundo Ingo Sarlet², a Lei Geral de Proteção de Dados teria assento numa

¹ MORAES, Maria Celina Bodin de. e QUEIROZ, Joao Quinelato de. Autodeterminação Informativa e responsabilização proativa: novos instrumentos de tutela da pessoa humana na LGDP, Proteção de dados pessoais: privacidade versus avanço tecnológico, **Cadernos Adenauer**, Vol. 3, Ano XX, 2019, p. 115.

² SARLET, Ingo Wolfgang. Proteção de Dados Pessoais como Direito Fundamental na Constituição Federal de 1988: contributo para a construção de uma dogmática constitucionalmente adequada, **Direitos**

miríade de direitos fundamentais que incluiriam não só a tutela da proteção dos dados em si, mas, também, os direitos à privacidade, liberdade, livre desenvolvimento da personalidade, dignidade da pessoa humana, intimidade e informação, previstos no art. 1º, inc. III c/c art. 5º, incisos II, X, XII e LXXII, da Constituição.

Segundo o autor, à época em que escrevera o artigo, o direito à proteção de dados poderia ser inferido do direito ao sigilo das comunicações de dados, da ação de *habeas data*, entre outros direitos fundamentais, conforme sintetiza o autor logo a seguir³:

À míngua, portanto, de expressa previsão de tal direito, pelo menos na condição de direito fundamental explicitamente autônomo, no texto da CF, e a exemplo do que ocorreu em outras ordens constitucionais, o direito à proteção dos dados pessoais pode (e mesmo deve!) ser associado e reconduzido a alguns princípios e direitos fundamentais de caráter geral e especial, como é o caso do princípio da dignidade da pessoa humana, do direito fundamental (também implicitamente positivado) ao livre desenvolvimento da personalidade, do direito geral de liberdade, bem como dos direitos especiais de personalidade mais relevantes no contexto, quais sejam – aqui nos termos da CF – os direitos à privacidade e à intimidade, no sentido do que alguns também chamam de uma “intimidade informática”. (grifos nossos)

Traçando um milimétrico percurso acerca da tutela jurídica da proteção de dados pelo ordenamento jurídico brasileiro, Danilo

Fundamentais & Justiça | Belo Horizonte, ano 14, n. 42, pp. 179-218, jan./jun. 2020.

³ *idem*, p. 184.

Donatela⁴ chama a atenção para a interpretação, sob magistério de Tércio Sampaio Ferraz Filho⁵, que a Corte Constitucional Brasileira conferira ao **sigilo da comunicação de dados – e não aos dados em si** – em decisão de 2006, “relatada pelo Ministro Sepúlveda Pertence,⁶ que, inclusive havia opinado favoravelmente em doutrina sobre a materialidade de um direito material sobre os dados pessoais, [mas que] não reconheceu a existência de uma garantia de inviolabilidade sobre dados armazenados em computador com base em garantias constitucionais.”

Independentemente desta diferenciação, recentemente, o Supremo Tribunal Federal, superando antigo paradigma da própria Corte, reconheceu o direito à proteção de dados pessoais e à *autodeterminação informacional*, destacado e independente do direito à privacidade, que exige não só uma garantia de abstenção do Estado em relação à esfera privada individual (inspirado no paradigma “*the right to be alone*”) em matéria de proteção de dados, **mas empodera o respectivo titular com medidas tendentes a consentir ou não, preservar, retificar e exigir que se mantenha a integridade de seus próprios dados, afastando-os de um controle estatal ubíquo** e de uma sociedade tecnológica que redunde num “fenômeno

⁴ DONATELA, Danilo. Panorama Histórico da Proteção de Dados Pessoais. In: DONEDA, Danilo. (Org.) **Tratado de Proteção de Direitos Pessoais**. Rio de Janeiro: Forense, 2021, p. 48.

⁵ FERRAZ JR., Tercio Sampaio. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado, **Revista da Faculdade de Direito da Universidade de São Paulo**, v. 88, p. 447, 1993.

⁶ Recurso Extraordinário 418-416-8/SC, 04.04.2006

comumente designado de *Ubiquitous Computing*".⁷

Com efeito, o Plenário do Supremo Tribunal Federal reconheceu a autonomia do direito fundamental à proteção de dados pessoais ao referendar a Medida Cautelar deferida pela Ministra Rosa Weber para suspender a eficácia da Medida Provisória n. 954/2020, que dispunha sobre o "*compartilhamento de dados por empresas de telecomunicações prestadoras de Serviço Telefônico Fixo Comutado e de Serviço Móvel Pessoal com a Fundação Instituto Brasileiro de Geografia e Estatística, para fins de suporte à produção estatística oficial durante a situação de emergência pública de importância internacional decorrente do coronavírus (Covid19), de que trata a Lei nº 13.979, de 6 de fevereiro de 2020*". (ADI 6.387/DF - proposta pelo Conselho Federal da OAB - e nas ADIs 6.388/DF, 6.389/DF, 6.390/DF e 6.391).

Esta decisão do STF — que reconheceu o direito fundamental autônomo à proteção de dados pessoais e o direito à *autodeterminação informativa* — está sendo considerada um marco histórico comparável àquela "famosa decisão do Tribunal Constitucional da então Alemanha Ocidental, de 1983, na qual foi declarada a inconstitucionalidade de dispositivos de uma lei que, à semelhança do caso brasileiro, criava um censo estatal e determinava a coleta de dados pessoais dos cidadãos para a otimização de políticas públicas. A decisão pioneira da Corte Constitucional alemã apontou para a necessidade de conceituação da divisão de poderes na nascente sociedade de informação

da época"⁸ e fixou o marco jurisprudencial da ***autodeterminação informacional (ou informativa)***.

No paradigma jurisprudencial brasileiro, a Relatora, Ministra Rosa Weber, em decisão ratificada pelo Plenário da Corte Suprema, destaca que **não existem mais dados neutros ou insignificantes, uma vez que qualquer dado que leve à identificação de uma pessoa pode ser utilizado para a formação de perfis informacionais que serão usados pelo Estado e por pessoas jurídicas de direito privado, de modo que todo e qualquer dado que leve à identificação de uma pessoa passa a merecer proteção constitucional, ainda mais se este dado esta sob a custódia do próprio Estado.**

Observe-se, porém, a título de ilustração, no que tange à comparação com o *case* paradigmático alemão, que Ingo Sarlet⁹ registrava, antes mesmo da referida decisão do STF, que:

Na sua multicitada decisão, o Tribunal Constitucional Federal alemão, contudo, não reconheceu diretamente um direito fundamental à proteção de dados pessoais, mas, sim, deduziu, numa leitura conjugada do princípio da dignidade da pessoa humana e do direito ao livre desenvolvimento da personalidade, um direito fundamental implícito à autodeterminação informativa, que, consiste, em suma e de acordo com o Tribunal, na prerrogativa de cada indivíduo de decidir em princípio e substancialmente

⁷ *idem*, pp. 179-180.

⁸ FERREIRA, Lúcia Maria Teixeira. A decisão histórica do STF sobre o direito fundamental à proteção de dados pessoais, **Conjur**, 25 Nov. 2020. Disponível em: <https://www.conjur.com.br/2020-nov-25/lucia-ferreira-stf-direito-protacao-dados-pessoais>. Acesso em: 15 Marc. 2021.

⁹ RLET, Ingo Wolfgang. *op. cit.*, p. 187.

sobre a divulgação e utilização de seus dados pessoais.

O próprio Tribunal Constitucional, contudo, na mesma decisão, alertou para o fato de que o direito à autodeterminação informativa não assegura a cada cidadão um controle absoluto sobre os seus dados, visto que, dada a inserção e responsabilidade comunitária e social do ser humano, este deve tolerar eventuais limitações do direito quando em prol do interesse geral.

Por ora, no Brasil, cingiu-se o Supremo Tribunal Federal ao reconhecimento da autonomia do direito fundamental à *autodeterminação informacional*, não tendo sido ainda instado a traçar seus limites. Neste sentido, cumpre ao Estado protegê-lo *per se*.

E, na medida em que o aumento da vigilância enfraquece a democracia, o compartilhamento de dados passa a exigir um ônus justificativo maior por parte do Estado, assim como a finalidade e adequação dos motivos que justificam a demanda de quem pretenda ter acesso ao conteúdo informacional do perfil de indivíduos cuja personalidade, afinal, se revela através deles, conforme argumentos igualmente veiculados pela Ministra Relatora.

Nota-se, pois, que o r. *decisum* da Alta Corte de Justiça brasileira se encontra em consonância com os princípios definidos na própria Lei Geral de Proteção de Dados, dos quais se passa a tratar logo adiante.

PARTE II - FUNDAMENTOS JURÍDICOS EM MATÉRIA DE PROTEÇÃO DE DADOS PESSOAIS NA LEI GERAL DE PROTEÇÃO DE DADOS

II.1. Da Aplicação da Lei Geral de Proteção de Dados ao Caso

A Lei Geral de Proteção de Dados (Lei Federal nº 13.709/2018 ou “LGPD”) é o marco regulatório da proteção de dados pessoais no Brasil, que regulamenta o tratamento das operações envolvendo dados pessoais, seja por meio digital ou não, dentro ou fora da *internet*. A lei trata, dentre outras questões, dos direitos dos titulares dos dados, das obrigações dos agentes de tratamento, do encarregado de dados, dos parâmetros para segurança da informação, dos requisitos para a transferência internacional de dados e, inclusive, das instruções quanto à atuação da Autoridade Nacional de Proteção de Dados (“ANPD”).

A LGPD **se aplica a qualquer pessoa física ou jurídica, de direito público ou privado**, que realize operações de tratamento (coleta, produção, recepção, classificação, processamento, etc.) de dados pessoais em território nacional, caso: (i) o tratamento tenha como objetivo a oferta ou fornecimento de bens ou serviços, (ii) o tratamento de dados seja de indivíduos em território nacional, ou ainda (iii) os dados pessoais tenham sido coletados em território nacional.

Importante frisar que a LGPD **não é aplicável** somente nos casos em que o tratamento dos dados pessoais seja realizado: (i) por pessoa física, para fins particulares e não comerciais; (ii) para fins exclusivamente jornalísticos, artísticos ou acadêmicos; (iii) pelo Poder Público, nas hipóteses de utilização para a promoção da segurança pública, da defesa nacional, da segurança do Estado ou de atividades de investigação e repressão de infrações penais; ou (iv) quando esses dados pessoais forem provenientes de fora do território nacional e não sejam objeto de comunicação, uso compartilhado de dados

com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência (desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto na lei).

Como se vê, não estando o caso em questão em qualquer das hipóteses de exclusão acima mencionadas, **a LGPD se aplica à matéria em questão.**

II.2. O compartilhamento de dados como hipótese de tratamento de dados: atração da LGPD

Na LGPD, o conceito de “tratamento de dados” é amplo, de forma a incluir toda operação realizada com dados pessoais – da coleta ao descarte, incluindo o mero armazenamento. A LGPD menciona expressamente diversos outros exemplos: coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Assim, a Lei se aplica a qualquer agente (pessoa física, jurídica ou órgão público) que realize o tratamento - termo definido no texto da Lei como **“toda operação realizada com dados pessoais”** -, compreendendo desde o simples acesso aos dados até o armazenamento, transferência, classificação, eliminação, ou qualquer outra manipulação desses dados pessoais, **a exemplo do compartilhamento de dados requerido pelo i. Tribunal de Contas do Município.**

Portanto, como o “compartilhamento de dados” ou eventual “autorização de acesso às bases de dados do Município pelo Tribunal de Contas do Município” se enquadra no conceito de “tratamento de dados”, também por essa razão a LGPD incide sobre o objeto desta consulta.

II.3. Principais Conceitos e Atores: O Município do Rio de Janeiro como Controlador responsável pelos dados dos contribuintes, que são Titulares de Dados com direitos previstos na LGPD

Para os fins da LGPD, **“dados pessoais”** são informações relacionadas a pessoas naturais direta ou indiretamente identificáveis. Dentro deste conjunto, os **“dados pessoais sensíveis”**, por sua vez, compõem uma categoria específica de informações pessoais que demandam maior grau de proteção legal diante do potencial discriminatório que pode derivar do seu tratamento.

Entram nesta lista aqueles dados pessoais sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dados referentes à saúde ou à vida sexual, ou ainda dado genético ou biométrico, quando vinculados a uma pessoa natural. Desse modo, enquanto o dado pessoal é aquele que pode identificar ou levar à identificação de alguém, o dado sensível além de identificar um indivíduo, é capaz de promover a sua discriminação. Note que um tratamento com dados pessoais que revele dados sensíveis também – ou com maior razão – está sujeito à proteção especial nos termos da lei.

Vale ressaltar que nesta dinâmica de tratamento de dados pessoais existem três atores fundamentais: o titular e os agentes de tratamento (controlador e operadores, respectivamente).

Titular: é a pessoa física a quem se referem os dados pessoais.

Controlador: é a empresa ou a pessoa jurídica ou física¹⁰ a quem compete a tomada de decisões em relação à forma e finalidade do tratamento desses dados.

Operador: é a empresa ou a pessoa jurídica ou física¹¹ que realiza o tratamento dos dados pessoais seguindo as ordens do controlador a partir da

escolha dos meios técnicos razoáveis para tanto.

A LGPD definiu os agentes de tratamento buscando identificá-los de acordo com o seu poder de decisão em relação ao tratamento dos dados pessoais.

Nesse sentido, de acordo com a legislação, aquele com poder de mando sobre os dados é o agente de tratamento que possui maior grau de responsabilidade perante o titular, respondendo diretamente por qualquer mau uso dos dados pessoais. Trata-se do Controlador (art 5º, inciso VI). Por sua vez, aquele que trabalha com os dados pessoais a mando do controlador recebe e denominação de Operador (art. 5º, inciso VII) e somente responde pelos danos causados na hipótese de ter agido de forma diferente daquela solicitada pelo controlador ou ilegalmente.

Como a LGPD tem como seu maior objetivo regular e proteger o tratamento dos dados pessoais da utilização não autorizada, o legislador, para organizar esta proteção, classificou os dados de diferentes níveis de acordo com o maior ou menor grau de exposição que o dado utilizado de forma indevida pode gerar ao seu Titular, bem como criou diferentes critérios para a responsabilização dos agentes de tratamento que se propõem a utilizar os dados pessoais de terceiros **dentro dos estritos limites autorizados**.

Sendo assim, como não há especificação dos dados requeridos, tampouco de sua sensibilidade, volume e riscos envolvidos, o Município deve presumir que as informações são altamente sensíveis e, por conseguinte, se preocupar com o compartilhamento de forma qualificada.

¹⁰ A LGPD faz remissão à Lei de Acesso à Informação (LAI) para englobar todos os órgãos e entidades da Administração Pública em seu escopo:

LGPD Art. 23:

Art. 23. O tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, desde que:

LAI

Art. 1º Esta Lei dispõe sobre os procedimentos a serem observados pela União, Estados, Distrito Federal e Municípios, com o fim de garantir o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal.

Parágrafo único. Subordinam-se ao regime desta Lei:

I - os órgãos públicos integrantes da administração direta dos Poderes Executivo, Legislativo, incluindo as Cortes de Contas, e Judiciário e do Ministério Público;

II - as autarquias, as fundações públicas, as empresas públicas, as sociedades de economia mista e demais entidades controladas direta ou indiretamente pela União, Estados, Distrito Federal e Municípios. (grifos nossos)

¹¹ *idem*

Como conclusão, vê-se que o Município do Rio de Janeiro, ao manter o **SISTEMA DE INTELIGÊNCIA FISCAL – SIF**, cujo banco de dados possui informações sigilosas e potencialmente sensíveis, figura no papel de **Controlador**, sendo responsável por dados pessoais e possivelmente por dados pessoais sensíveis, estando o Tribunal de Contas do Município a postular a posição de **Controlador** de tais dados também.

II.4. Bases Legais para o Tratamento de Dados Pessoais

Para resumir, foi estabelecido, como regra geral (Art. 1º), que qualquer pessoa que trate dados, seja ela natural ou jurídica, de direito público ou privado, inclusive na atividade realizada nos meios digitais, deverá ter uma **base legal** para fundamentar os tratamentos de dados pessoais que realizar. Isso importa dizer que não haverá necessidade de identificação de uma base legal apropriada apenas nos casos que se enquadrarem nas hipóteses de exclusão de aplicação da lei previstas no Art. 4º da LGPD, mas também nas que autorizem expressamente o seu valimento.

Mas, ainda assim, o tratamento de dados pessoais previsto no Art.4º, inciso III (para fins exclusivos de segurança pública; defesa nacional; segurança do Estado; ou atividades de investigação e repressão de infrações penais) "será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei". Para tanto, já foi criada no âmbito da Câmara dos Deputados, Comissão de

Juristas responsável pela elaboração de anteprojeto de lei sobre essa matéria.

Portanto, não sendo uma hipótese de exclusão, deverá ocorrer o encaixe do tratamento realizado em pelo menos uma das hipóteses legais para que ele seja considerado legítimo e lícito. Essas bases foram estipuladas de forma geral e variada, devendo detalhes e especificações ser realizadas especialmente pela Autoridade Nacional de Proteção de Dados (ANPD), pelo Legislativo e Judiciário.

Nesta toada, com o intuito de garantir que o tratamento de dados pessoais seja válido e lícito, a LGPD prevê um rol de hipóteses em que estas operações poderão ocorrer. Estas condições legais, mais conhecidas como "Bases Legais", abarcam diferentes cenários possíveis para a legitimação das operações de tratamento previstas nos artigos 7º e 11 da LGPD, segundo os quais os dados pessoais só podem ser tratados:

1. Mediante o fornecimento do **consentimento do titular**; e para
2. Atender aos **interesses legítimos** do controlador ou de terceiro;
3. O **cumprimento de obrigação legal ou regulatória** pelo controlador;
4. A **execução de contrato ou de procedimentos preliminares** relacionados a contrato do qual seja parte o titular;
5. O **exercício regular de direitos em processo** judicial, administrativo ou arbitral;
6. A **proteção do crédito**;
7. A **proteção da vida ou da incolumidade física** do titular ou de terceiro;

8. A **tutela da saúde** (apenas por profissionais de saúde, serviços de saúde ou autoridade sanitária);

9. A **realização de estudos por órgão de pesquisa**; e

10. A **execução de políticas públicas** (apenas pela Administração Pública), observados os requisitos legais.

No caso do tratamento de dados pessoais pelo Poder Público, deve-se observar: (i) o atendimento de sua finalidade pública, (ii) a persecução do interesse público, (iii) o objetivo de executar as competências legais (iv) ou de cumprir as atribuições legais do serviço público, desde que:

Art. 23 *in omissis*;

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

III - seja indicado um encarregado quando realizarem operações de tratamento de dados pessoais, nos termos do art. 39 desta Lei; e (Redação dada pela Lei nº 13.853, de 2019) Vigência

A lei também admite o compartilhamento de dados entre órgãos públicos para (iv) o atendimento específico (v) de execução de políticas públicas (art. 26), desde que, obedecidas todas essas regras, sejam também

seguidos (vi) os princípios do art. 6º da LGPD, quais sejam:

Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:

I- finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

II- adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

III- necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

V- qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

VII- segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

IX- não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

X- responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

A prestação de serviços públicos e formulação e execução conjunta de políticas públicas é, inequivocamente, uma das principais hipóteses que demanda o tratamento de dados pessoais pelo Estado e, por consequência, desafia a advocacia pública na definição das orientações jurídicas aplicáveis, à luz da LGPD.

O Município do Rio de Janeiro, na qualidade de Controlador, tem a responsabilidades de avaliar o enquadramento de ao menos uma das bases legais para a realização de cada tratamento de dados pessoais (artigo 7º, para dados pessoais, e artigo 11, para dados sensíveis, c/c art. 23 ou 26 da LGPD), bem como de verificar a presunção de possibilidade de compartilhamento de bases de dados entre pessoas jurídicas de direito público, salvo as cobertas por sigilo fiscal, respeitados os princípios de proteção de dados estabelecidos em seu art. 6º, bem como as exceções legais à vedação genérica de compartilhamento de bases de dados a que tenha acesso com entidades privadas (art. 26), conforme recentemente tratado na Manifestação Técnica PG/PADM/CT/0231/2021/AFC.

O tema das bases legais de tratamento de dados pessoais de que pode se valer o Poder Público já vem suscitando significativas dúvidas práticas e controvérsias

doutrinárias¹². Cuida-se de debate ainda incipiente e pendente de maior conformação pela Autoridade Nacional de Proteção de Dados (ANPD). Nesse cenário, no item abaixo, apresentam-se os principais casos em que o Poder Público realizará o tratamento de dados pessoais com esteio em ‘bases legais’.

II.5. Principais bases legais aplicadas ao Poder Público

Em matéria de tratamento de dados pessoais pelo Estado, há que se destacar as duas bases legais previstas na LGPD que guardam maior afinidade com o agir administrativo: cumprimento de obrigação legal ou regulatória (arts. 7º, II, e 11, II, “a”) e execução de políticas públicas (arts. 7º, III, e 11, II, “b”).

Primeiramente, parece necessário partir da superação da visão tradicional da matéria dos serviços públicos, que a analisa a partir da posição jurídica do Estado em detrimento da dos cidadãos, passando-se a compreender a prestação de serviços públicos não mais como uma prerrogativa (exclusiva) do Estado, mas como verdadeira obrigação que lhe é imposta pelo ordenamento jurídico para a promoção e efetivação de determinado direito fundamental que assiste ao cidadão.

Vale dizer, a atribuição da natureza de serviço público a dada atividade produz como consequência jurídica a criação ao Estado do dever de oferecê-la à comunidade de modo permanente, regular e a um custo acessível. Neste sentido, a viabilidade jurídica do tratamento de dados pessoais dos usuários de serviços públicos decorreria exatamente do enquadramento da prestação dos serviços

¹² Confira-se, dentre outros: DONEDA, Danilo. (Org.) **Tratado de Proteção de Direitos Pessoais**. Rio de Janeiro: Forense, 2021,

públicos – e aqui supostamente dos meios indispensáveis a concretizá-los – como *obrigação legal/constitucional* imputável ao Estado, descerrando-se a aplicabilidade da base legal prevista nos arts. 7º, II, e 11, II, “a”, da LGPD.

Ademais, parece plenamente viável que, em certos casos, a prestação de serviços públicos, qualificável como obrigação legal/constitucional do Estado, possa ser igualmente objeto de uma *política pública em execução*, tangenciando, simultaneamente, as duas bases legais de tratamento de dados pessoais previstas nos arts. 7º, II e III, e 11, II, “a” e “b”, da LGPD, muito embora o conceito de política pública tenha assumido um espectro tão lato de modo a abarcar atos administrativos infra legais absolutamente desconectados de uma estrutura prévia de planejamento e d’ outra, de monitoramento, pelo quê há que se ter uma definição bem precisa de seu conceito para que não signifique todo e qualquer agir administrativo.

Afigura-se igualmente viável que, em hipóteses específicas, determinadas políticas públicas, em razão do seu estágio de desenvolvimento e implementação, não envolvam efetiva e concretamente o adimplemento de uma obrigação estatal materializada na prestação de um serviço público em favor da comunidade, caso em que será possível uma separação entre as supracitadas bases de tratamento de dados pessoais.

Indo além, cabe sublinhar a previsão do art. 23 da LGPD, que disciplina o tratamento de dados pessoais por pessoas jurídicas de direito público de forma complementar às dos arts. 7º e 11, o qual deve ser realizado para

“(i) atendimento de sua finalidade pública, (ii) na persecução do interesse público, (iii) com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público”, o que revela uma série de outros requisitos que devem ser cumpridos e que virão a ser elencados no caso específico deste processo, que cuida da proteção de dados fiscais, tais como: (i) necessidade de motivação específica; (ii) finalidade de controle que é legalmente conferida à Corte de Contas; e (iii) imprescindibilidade da exposição dos motivos que suscitam o pedido de compartilhamento de dados, (iv) devendo ser observado o *devido processo legal administrativo*.

Há quem vislumbre no art. 23 da LGPD uma **base legal de tratamento autônoma para os serviços públicos**, os quais não estariam abrangidos, em toda a sua amplitude, pelas bases legais dos arts. 7º e 11 da LGPD, o que não me parece condizente com a proteção constitucional que se pretende conferir ao direito fundamental à *autodeterminação informacional*. Todavia, parcela significativa da doutrina vem entendendo que o art. 23 da LGPD não apresenta um conteúdo verdadeiramente emancipatório em relação às bases legais previstas nos arts. 7º e 11 da LGPD, que, como visto, se aplicam plenamente em tema de serviço público.

Trata-se de conclusão que pode ser depreendida dos próprios termos utilizados pela LGPD para qualificar as supracitadas normas. Enquanto os arts. 7º e 11 são designativos das “hipóteses” em que poderá ser legalmente realizado o tratamento de dados pessoais, constituindo “requisito” legal para o tratamento, o art. 23 fixa as “regras”

que deverão ser observadas por pessoas jurídicas de direito público no exercício de tal atividade.

Conclui-se, portanto, que o tratamento de dados pessoais no âmbito da prestação de serviços públicos é viável diante da fundamentação em uma das bases legais da LGPD, sendo possível a incidência tanto da hipótese prevista nos arts. 7º, II, e 11, II, “a”, relativa ao cumprimento de obrigação legal, quanto da disciplinada nos arts. 7º, III, e 11, II, “b”, concernente às políticas públicas, os quais são taxativos, apesar de dotados de hipóteses dotadas de cláusulas abertas e com certo grau de subjetividade (como, por exemplo, o legítimo interesse).

Em ambos os casos, dispensa-se, em teoria, a obtenção de consentimento. Acrescentem-se a elas apenas as hipóteses a que faz alusão indireta a LGPD, quando faz remissão à LAI. (art. 31, §3º, inc. I a V, da Lei Federal n. 12.527/2011).

De todo modo, é certo que o compartilhamento de dados pelo Poder Público demanda a observância às regras previstas nos arts. 23 a 32 da LGPD, bem como o atendimento aos princípios incidentes na hipótese, sobretudo no que tange aos princípios previstos no art. 6º da LGPD.

II.5. Princípios gerais e melhores práticas são igualmente aplicáveis ao Poder Público

A LGPD estabelece alguns princípios que se aplicam a todas as atividades de tratamento de dados. São valores gerais que orientam a compreensão, interpretação e aplicação das regras estabelecidas pela LGPD e que devem sempre ser considerados quando uma atividade envolver tratamento

de dados pessoais. Entre os princípios mais relevantes, estão os seguintes: ***princípios da finalidade, adequação e necessidade.***

De acordo com esses princípios, dados pessoais só devem ser coletados e tratados para os propósitos específicos e legítimos que tenham sido informados ao titular de dados e sejam compatíveis com o contexto do tratamento. O tratamento deve ser limitado ao mínimo necessário para aquelas finalidades que foram informadas aos titulares. Isso significa que antes de coletar, armazenar ou de qualquer maneira utilizar dados pessoais – a exemplo do compartilhamento –, é importante verificar:

- i. se o titular daqueles dados foi informado de maneira clara e específica sobre como os dados serão tratados e para quais finalidades – o porquê do tratamento;
- ii. se o tratamento é adequado ao contexto em que os dados foram coletados, ou seja, às expectativas que o titular de dados tinha ao fornecer os seus dados ou torná-los disponíveis; e
- iii. se é realmente necessário tratar aqueles dados para atingir aquela finalidade.

Todos esses princípios repercutem sobremaneira no tema da consulta – Compartilhamento de Dados Pessoais com o Poder Público –, haja vista que os órgãos públicos devem estar adequados à LGPD, dando atenção às diversas mudanças de interpretação constitucional e legislativas relacionadas ao tema e tendo como eixo fundamental as bases legais previstas no art. 7º e 11 da Lei, os princípios disciplinados no art. 6º, bem como todo o Capítulo IV da LGPD.

II.6. Responsabilidade dos agentes de tratamento e dos servidores públicos em relação ao tratamento de dados pessoais

A LGPD trata do regime de responsabilidade civil e ressarcimento de danos aplicável aos agentes de tratamento que violem a lei nos artigos 42 ao 45. De acordo com a norma (art. 42), a responsabilidade pelo tratamento de dados é integralmente do Controlador, devendo o operador ser responsabilizado de forma solidária em caso de descumprimento da lei ou das instruções lícitas recebidas do Controlador.

Neste contexto, será considerado tratamento irregular de dados (art. 44), ou seja, passível de responsabilização, o tratamento que deixar de observar a LGPD ou ainda que não fornecer a segurança de proteção que o titular poderia esperar, considerando o modo como o tratamento é realizado, os riscos razoáveis que se pode esperar e a técnica de tratamento aplicada à época em que o tratamento foi realizado.

Portanto, o Controlador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo. Todos os Controladores diretamente envolvidos em operação de tratamento de dados, que causem dano ao titular, serão solidariamente responsáveis, salvo se: (i) não realizaram o tratamento dos dados pessoais que lhes foram atribuídos; (ii) apesar de terem realizado o tratamento dos dados pessoais que lhes foram atribuídos, não houve violação da lei de proteção de dados; ou (iii) o dano decorrer de culpa exclusiva do titular dos dados ou de terceiro.

Desta forma, descumprida quaisquer das obrigações legais ou contratuais, o Controlador responde pela reparação de danos. Ademais, na hipótese de haver mais de um controlador envolvido no tratamento de dados, a responsabilidade dos envolvidos é também solidária, cabendo o direito de regresso entre eles.

Vale mencionar, ainda, que o **tratamento de dados pessoais será irregular** quando não observar a legislação (não se enquadrando em alguma das autorizações acima mencionadas) ou quando não fornecer a segurança que o titular pode esperar, considerando: (i) o modo pelo qual o tratamento é realizado; (ii) o resultado e os riscos que razoavelmente dele se esperam; e (iii) as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado.

Uma vez que a operação de tratamento não for capaz de se enquadrar mais em alguma das bases legais previstas em lei, o controlador deverá promover o **término do tratamento**, o que ocorrerá quando: (i) o período do tratamento chegar ao fim; (ii) ocorrer uma manifestação do titular dos dados solicitando o término do tratamento; (iii) houver determinação legal nesse sentido; ou (iv) for verificado que a finalidade que fundamentou o tratamento foi alcançada ou que os dados pessoais coletados perderam a sua pertinência para a finalidade pretendida.

No caso em apreço, todavia, se a responsabilidade do servidor se torna ainda mais suscetível de controle, o consentimento do Titular dos dados passa a ser irrelevante para o Fisco-Controlador, uma vez que sobre o direito à autodeterminação informacional

prevalecerá o direito da coletividade a que não haja fraude ao Fisco, conforme já teve oportunidade de julgar o STF em matéria de proteção de dados cobertos por sigilo fiscal, como se verificará na Parte III desta Manifestação.

Por fim, vale mencionar o capítulo da LGPD que diz respeito à fiscalização e à responsabilidade no tocante ao Poder Público. Há que se mencionar que o art. 29 está disposto no contexto da Seção I da LGPD, ao passo que os arts. 31 e 32 estão inseridos na Seção II.

O art. 29 expressa que a ANPD poderá solicitar, a qualquer momento, aos órgãos e às entidades do poder público a realização de operações de tratamento de dados pessoais, informações específicas sobre o âmbito e a natureza dos dados e outros detalhes do tratamento realizado e poderá emitir parecer técnico complementar para garantir o cumprimento da Lei.

O art. 31 preconiza que quando houver infração à LGPD em decorrência do tratamento de dados pessoais por órgãos públicos, a Autoridade Nacional poderá enviar informe com medidas cabíveis para fazer cessar a violação. Além disso, conforme estabelece o art. 32, a ANPD poderá solicitar a agentes do Poder Público a publicação de relatórios de impacto à proteção de dados pessoais e sugerir a adoção de padrões e de boas práticas para os tratamentos de dados pessoais pelo Poder Público.

Vislumram-se nesses dispositivos a base legal para a eventual responsabilização pessoal dos servidores públicos cujas condutas se enquadrem na Lei de Improbidade Administrativa. Também por estas razões, o Município do Rio de Janeiro,

como Controlador de dados, deve respeitar procedimentos específicos para o compartilhamento de dados, inclusive para assegurar a legalidade das ações dos servidores públicos de seus quadros administrativos.

É relevante, pois, quando haja a possibilidade do compartilhamento de dados *in genere* – excluída a matéria fiscal –, que se exijam relatórios de impacto à proteção de dados pessoais, seja o operador, ou eventualmente um “cooperador”, pessoa jurídica de direito público ou privado, este a favor da qual não milita a presunção legal de cabimento, observados os requisitos legais, mas antes o de vedação, a não ser que verificadas determinadas exceções expressamente previstas na LGPD.

No caso de dados pessoais cobertos por sigilo fiscal, o compartilhamento com a iniciativa privada deve restar proscria em razão da disciplina específica tratada na Parte III desta Manifestação Técnica.

II.7. O tratamento de dados pessoais pelo Poder Público e os principais aspectos jurídicos para a elaboração de um convênio/instrumento congênere para o compartilhamento de dados pessoais

O art. 23 da LGPD correlaciona a norma com a Lei Federal no 12.527/11, a denominada *Lei de Acesso à Informação – a LAI*. O mencionado diploma legal, em seu art. 1o, dispõe sobre os procedimentos a serem observados pela União, Estados, Distrito Federal e Municípios, com o fim de garantir acesso à informação previsto no inciso XXXIII do art.5º, no inciso II do §3º do art. 37 e no §2º do art. 216, todos da CRFB/88,

salientando-se que o parágrafo único estabelece que se subordinam ao respectivo regime jurídico: (i) órgãos públicos integrantes da administração direta dos Poderes Executivo, Legislativo, incluindo as **Cortes de Contas**, e Judiciário e do Ministério Público; e (ii) as autarquias, as fundações públicas, as empresas públicas, as sociedades de economia mista e demais entidades controladas direta ou indiretamente pela União, Estados, Distrito Federal e Municípios.

Dessa forma, a LGPD engloba em seu escopo as mesmas entidades listadas na Lei de Acesso à Informação, cabendo ao *caput* do art. 23 prever que o tratamento por tais órgãos e pessoas deva ser realizado para o atendimento de sua finalidade pública, persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público.

Observe-se que o art. 23, §3º, da LGPD também se refere ao respeito ao exercício dos direitos do titular de informações perante o Poder Público de acordo com a Lei de Acesso à Informação, que, em seu art. 31, reafirma que o tratamento das informações pessoais deve ser feito de forma transparente e com respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais e que só podem “ter autorizada sua divulgação ou acesso por terceiros diante de previsão legal ou consentimento expresso da pessoa a que elas se referirem” (art. 31, §1º, inc. II), sendo responsabilizado aquele que der causa ao seu uso indevido (art. 31, § 2º), salvo, confira-se:

Art. 31 *in omissis*;

§ 3º O consentimento referido no inciso II do § 1º não será exigido quando as informações forem necessárias:

I- à prevenção e diagnóstico médico, quando a pessoa estiver física ou legalmente incapaz, e para utilização única e exclusivamente para o tratamento médico;

II - à realização de estatísticas e pesquisas científicas de evidente interesse público ou geral, previstos em lei, sendo vedada a identificação da pessoa a que as informações se referirem;

III- ao cumprimento de ordem judicial;

IV - à defesa de direitos humanos; ou

V- à proteção do interesse público e geral preponderante.

Neste sentido, **parece-me que as políticas públicas que autorizam o compartilhamento de dados pelo Poder Público, além da observância aos requisitos de forma previstos na LGPD (requisitos do art. 6º, previsão em lei ou atribuição legal do caput do art. 23 e observância ao devido processo legal administrativo) e que dispensam o consentimento do titular dos dados, devem ser interpretadas, nas hipóteses “abertas”, de acordo com o art. 31, §3º, inc. IV e V, da LAI, no sentido de dizer respeito à defesa de direitos humanos ou à proteção do interesse público e geral preponderante.**

Como sempre, a Administração Pública deve demonstrar, motivar e justificar a aplicabilidade casuística de “cláusulas jurídicas” e conceitos jurídicos com conteúdo *abstramente indeterminado*, como “política pública”, “interesse público e geral preponderante” e “direitos humanos”, mas *determináveis* no caso concreto, sob pena de o direito à *autodeterminação informacional* do titular de dados sob custódia do Estado nunca

desfrutar de eficácia, tampouco de efetividade constitucional.

O setor público, assim como o setor privado, também se submete às normas da LGPD, nos termos do Capítulo IV da Lei. Conforme mencionado acima, as únicas exceções estão previstas no art. 4º, inciso III, que afastam a incidência da LGPD quando o tratamento de dados pessoais for realizado para fins exclusivos de: segurança pública; defesa nacional; segurança do Estado; ou **atividades de investigação e repressão de infrações penais**. Todavia, mesmo nessas hipóteses excludentes – que serão objeto de uma legislação específica – deverão ser observados, pelo Poder Público, medidas proporcionais e estritamente necessárias ao atendimento público, **observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos na LGPD.**

II.8. Considerações finais e recomendações para um compartilhamento de dados (em abstrat) que respeite a LGPD

Todas as recomendações adotadas estão fundamentadas no conceito da proteção de dados pessoais baseada em análises contextuais do risco – *risk-based approach*, o que determina que **os programas de governança e compliance sejam efetivamente mensurados e calibrados com fundamento nos riscos aos indivíduos**, cabendo ressaltar que a LGPD considera irregular o tratamento de dados pessoais que não protege os **indivíduos** de acordo com os riscos relacionados a esse tratamento (art. 44).

Nestes termos, ao analisar um compartilhamento massivo de dados

personais dos contribuintes com diversos órgãos do Poder Público, deve-se levar em consideração, principalmente, o enorme volume de dados pessoais que estão sendo transferidos, a regularidade e legalidade dessas transferências e a probabilidade e gravidade dos riscos aos titulares de dados. Trata-se de uma decisão de alto risco no contexto da proteção de dados pessoais e que pode, inclusive, repercutir na esfera jurídica privada dos envolvidos.

Diante de todo o exposto, é importante destacar que **a estruturação de eventuais convênios/instrumentos congêneres com o Poder Público exige especial cautela e uma eventual comprovação em procedimento administrativo, por ambas as partes, da precaução e das boas práticas adotadas (ex ante) exigidas pela LGPD.**

Ademais, estes instrumentos exigirão um alto nível de transparência em seus Avisos e Políticas de Privacidade/Proteção de Dados Pessoais junto aos titulares de dados, que deverão ser comunicados acerca desse compartilhamento e, em alguns casos, deverão fornecer o seu consentimento, o que, repita-se, **não é o caso concreto de que ora se cuida, por se tratar de dados pessoais cobertos por sigilo fiscal, que já relativizavam a autodeterminação informacional** antes mesmo de ela ter reconhecida sua autonomia na ordem constitucional brasileira pelo Supremo Tribunal Federal, de acordo com v. **acórdãos da própria Corte Constitucional brasileira.**

Em relação ao direito dos titulares em **matéria não fiscal relacionada à LGPD,** embora dependa de regulamentação específica pela ANPD, os prazos e

procedimentos para exercício dos direitos dos titulares deverão ser gratuitos e de fácil acesso, havendo a tendência de que sejam disponibilizados no sítio eletrônico das instituições. Isto demanda uma estrutura organizacional complexa que será afetada pelas ações de compartilhamento de dados, razão pela qual devem ter sinergia e ser analisadas pelo Encarregado.

Outrossim, recomenda-se doravante a realização de **Relatório de Impacto à Proteção de Dados - RIPD**, por se tratar da mais importante ferramenta do modelo de gerenciamento de riscos e de conformidade com a Lei, nas hipóteses de compartilhamentos de dados não fiscais que exigirem análise por parte desta Procuradoria Administrativa, uma vez que esta Parte II desta Manifestação Técnica também teve uma pretensão de análise abstrata da LGPD.

No plano prático, recomenda-se também que seja avaliado o melhor instrumento jurídico para a hipótese, caso, no futuro, venha a ser possível o compartilhamento diante: (i) de uma finalidade específica; (ii) com vistas à execução de uma política pública; (iii) do interesse público municipal, no caso concreto, após analisados os requisitos impostos ao final da Parte III deste pronunciamento.

Em relação ao instrumento jurídico que permitirá o acesso ao banco de dados ou acesso a informações pelo Poder Público, o princípio da legalidade é o guia para a atuação dos agentes. Isso significa que a decisão (i) dependerá da finalidade (específica) e do regime aplicável à "guarda" dos dados; (ii) deverá ser formalizada em procedimento

administrativo; (iii) devendo ser evitados pedidos genéricos e sem indicação de finalidade específica, como no caso em tela, razões para o pedido e os responsáveis (Encarregados); (iv) havendo o ônus de demonstração, pelo Poder Público, de que o requerente não precisa de autorização da ANPD para realizar o compartilhamento, quando se tratar de pessoa jurídica de direito privado.

Além das cautelas supracitadas, **destacam-se os seguintes aspectos que também devem orientar a formulação de convênios e instrumentos congêneres de compartilhamento de dados** com o Poder Público:

- a) exposição clara sobre os tipos de dados que serão compartilhados e as finalidades específicas buscadas;
- b) acesso norteado pela finalidade específica e legalidade do referido compartilhamento de dados;
- c) indicação precisa do disposto no inciso I do art. 23 da LGPD e da base legal que legitimaria o tratamento de dados pessoais pelo Poder Público e a transferência de dados em tela;
- d) papel dos convenientes como agentes de tratamento,;
- e) contrapartidas e responsabilidades do Poder Público, como controlador, diante das exigências da LGPD;
- f) indicação do Encarregado/DPO do órgão público;
- g) medidas de segurança adotadas, nos termos das melhoras práticas e das normas técnicas de segurança;
- h) salvaguardas necessárias em relação à privacidade e à proteção dos dados

personais que o Ente Público eventualmente irá compartilhar;

i) inclusão de cláusulas de auditoria;

j) procedimento para atendimento às requisições de titulares de dados e demais direitos previstos na LGPD; entre outras disposições-padrão;

k) indicação de que não serão compartilhados dados sensíveis e de crianças/adolescentes, salvo nas hipóteses específicas de legislação autorizadora, com as cautelas de praxe.

A entrada em vigor da LGPD causou, e ainda causará, um enorme impacto na forma como são utilizados os dados pessoais dos indivíduos. Apesar de recorrente, é errada a ideia de que a LGPD é a única legislação que versa sobre como devem ser utilizados os dados pessoais pelos Poderes Públicos depois de seu advento; sua transversalidade e tentacularidade se espalha por milhares de contratos, convênios e ajustes celebrados no âmbito da Administração Pública, sem que ela disso se dê conta, mas isso não afasta a incidência, outrossim, das legislações específicas de regência dessas relações jurídicas, com as quais a LGPD deverá ser permanentemente conjugada.

O panorama jurídico brasileiro de privacidade e proteção de dados é ainda complexo e conta com leis setoriais específicas, ao lado do **marco regulatório genérico da proteção contra a sociedade ubíqua**. A LGPD deve ser entendida e interpretada como parte de um sistema e não como uma lei isolada. Portanto, ao tratar de proteção de dados no Brasil, deve-se garantir a observância de diversas leis, a exemplo da legislação tributária.

É o que se passa a expor.

PARTE III - FUNDAMENTOS JURÍDICOS EM MATÉRIA DE PROTEÇÃO DE DADOS PESSOAIS COBERTOS POR SIGILO FISCAL

Os direitos à privacidade, à proteção de dados, à personalidade, que da produção de dados também advém, ao resguardo da imagem do contribuinte, de cujos dados fazendários o Fisco pode esboçar um retrato, ainda que parcial, do sujeito, à liberdade, à *autodeterminação informacional*, são direitos fundamentais e, neste sentido, oponíveis ao Estado.

Segundo o Supremo Tribunal Federal, “do ponto de vista da autonomia individual, o sigilo bancário é uma das expressões do direito de personalidade que se traduz em ter suas atividades e informações bancárias livres de ingerências ou ofensas, qualificadas como arbitrárias ou ilegais, de quem quer que seja, inclusive do Estado ou da própria instituição financeira.” (Recurso Extraordinário nº 601.314)¹³.

Não sendo absolutos, porém, os valores que o sigilo bancário protege, comportam exceções, como as que visam a preservar indene de fraudes a Fazenda Pública e, de resto, a sociedade; nesta qualidade, devem ser interpretadas restritivamente.¹⁴

¹³ Nota-se que se trata de decisão anterior àquela que reconheceu a autonomia do direito à liberdade informacional, mas que já cotejava todos os direitos fundamentais dos quais ela defluía, enquanto direito à proteção/sigilo do dado fiscal, com o do Fisco a a eles ter acesso de modo a preservar o princípio tributário da redistribuição. Mas apenas o Fisco.

¹⁴ Em matéria tributária, o Supremo Tribunal Federal já teve oportunidade de se manifestar no sentido de permitir à Fazenda Pública o acesso a dados bancários para fins de persecução penal, conforme se verificará mais adiante. De acordo com a lei, Fazenda Pública engloba os Entes Federativos e suas Autarquias e Fundações de Direito Público, não podendo ampliar seu alcance mediante interpretação extensiva para

Neste sentido, o sigilo fiscal é meio de promoção do **direito à personalidade, à privacidade e à proteção de dados**, instituídos no art. 1º, inc. III c/c art. 5º, inc. II, X e XII, da Carta Magna e, sendo assim, firmado no **interesse do cidadão-contribuinte vis-à-vis ao da coletividade, de cujos impostos, calcados na capacidade contribuinte dos indivíduos, depende para que o Estado atenda à satisfação do interesse comum, na forma do art. 145, §1º, da Constituição.**

O **artigo 198 do Código Tributário Nacional** estabelece que seja vedada a divulgação, por parte da Fazenda Pública ou de seus servidores, de informação obtida em razão do ofício sobre a situação econômica ou financeira do sujeito passivo ou de terceiros e sobre a natureza e o estado de seus negócios ou atividades, com vistas ao resguardo desses direitos fundamentais. §

As exceções encontram-se nos seus parágrafos primeiro e terceiro. A principal delas diz respeito à requisição de autoridade judiciária no interesse da Justiça. Da mesma forma, é possível a divulgação de informações relativas a representações fiscais para fins penais; inscrições em dívida ativa e informações relativas a parcelamento ou moratória.

Art. 198. Sem prejuízo do disposto na legislação criminal, é vedada a divulgação, por parte da Fazenda Pública ou de seus servidores, de informação obtida em razão do ofício sobre a situação econômica ou financeira do sujeito passivo ou de terceiros e sobre a natureza e o estado de seus negócios ou atividades.

alcançar os órgãos de controle externo da Administração Pública, como Tribunais de Contas e Ministério Público.

§ 1º Excetuam-se do disposto neste artigo, além dos casos previstos no art. 199, os seguintes:

I – requisição de autoridade judiciária no interesse da justiça;

II – solicitações de autoridade administrativa no interesse da Administração Pública, desde que seja comprovada a instauração regular de processo administrativo, no órgão ou na entidade respectiva, com o objetivo de investigar o sujeito passivo a que se refere a informação, por prática de infração administrativa.

§ 2º O intercâmbio de informação sigilosa, no âmbito da Administração Pública, será realizado mediante processo regularmente instaurado, e a entrega será feita pessoalmente à autoridade solicitante, mediante recibo, que formalize a transferência e assegure a preservação do sigilo.

§ 3º Não é vedada a divulgação de informações relativas a:

I – representações fiscais para fins penais;

II – inscrições na Dívida Ativa da Fazenda Pública;

III – parcelamento ou moratória.

Art. 199. A Fazenda Pública da União e dos Estados, do Distrito Federal e dos Municípios prestar-se-ão mutuamente assistência para a fiscalização dos tributos respectivos e permuta de informações, na forma estabelecida, em caráter geral ou específico, por lei ou convênio.

Parágrafo único. A Fazenda Pública da União, na forma estabelecida em tratados, acordos ou convênios, poderá permutar informações com Estados estrangeiros no interesse da arrecadação e da fiscalização de tributos. (grifos nossos)

Como destacado na PG/4ª PS/006-RARS, as solicitações **que digam respeito ao fornecimento de dados não individualizados** (ex: base legal para a

concessão de imunidades e isenções; os valores totais que deixaram de ser arrecadados anualmente em virtude de eventual isenção ou imunidade) podem ser fornecidos, pois tratam de dados gerenciais relativos à Administração Fazendária Municipal sobre os quais há amplo poder de controle, interno e externo, além evidentemente de estarem sujeitos ao princípio da publicidade.

Nesse sentido, na **Manifestação Técnica PG/PADM/T/008/2020/PRSM**, aprovada pela Chefia da PADM e a Chefia da SUBCONS, restou consignada a **possibilidade de prestação de dados gerenciais sem informações dos devedores**. Ao final, pela Chefia da SUBCONS, foi sugerida a criação de códigos (ou inscrições) correspondentes às inscrições fiscais ou imobiliárias como solução a viabilizar o fornecimento *desidentificado* de informações sigilosas:

Ementa da MT
PG/PADM/T/008/2020/PRSM
DIREITO TRIBUTÁRIO. DADOS PARA A SECURITIZAÇÃO DOS CRÉDITOS DA DÍVIDA ATIVA E COBRANÇA ADMINISTRATIVA. DÉBITOS NÃO PARCELADOS NEM INSCRITOS EM DÍVIDA ATIVA. SIGILO FISCAL. IMPOSSIBILIDADE DE IDENTIFICAÇÃO DOS CONTRIBUINTES (ARTIGO 198 DO CTN). POSSÍVEL A PRESTAÇÃO DE DADOS GERENCIAIS SOBRE OS DÉBITOS, SEM AS INFORMAÇÕES DOS DEVEDORES.

Fragmento do Visto SUBCONS:

APROVO a Manifestação Técnica PG/PADM/T/NS 008B/2020/PRSM, que mereceu o visto favorável da I. Chefia da PG/PADM, em detrimento da manifestação divergente da I. Assessoria desta PG/SUBCONS.

Ainda que não esteja expresso na Constituição Federal, o sigilo fiscal fundamenta-se e surge como desdobramento dos direitos constitucionais a inviolabilidade da intimidade e da vida privada das pessoas físicas e jurídicas, impedindo a Administração Tributária de divulgar informações fiscais de contribuintes e terceiros. Assim é que, a mesma Constituição Federal que prestigia como princípio geral a publicidade e a transparência ressalva a garantia de proteção a privacidade e intimidade.

As exceções ao sigilo fiscal encontram-se integralmente previstas em lei, tratando-se sempre, de transferência de dados e informações entre Fazendas Públicas, Poderes (Judiciário ou Legislativo) e Ministério Público. Nestas hipóteses, o dever de sigilo, por força de lei, é transferido ao Órgão ou Poder receptor das informações. Não há exceção ao sigilo fiscal que envolva entidade privada.

Nada obsta, entretanto, que a Secretaria de Fazenda crie códigos (ou inscrições) correspondentes as inscrições fiscais ou imobiliárias, relacionadas ao contribuinte ou ao seu patrimônio, com a finalidade de fornecer, de forma desidentificada, os dados necessários para que o contratado execute de forma eficiente e otimizada o objeto contratual, sem violar o dispositivo legal que impõe sigilo sobre a identificação do sujeito passivo, enquanto não inscrito o crédito em dívida ativa.

A complexa questão acerca do sigilo foi enfrentada mais de uma vez pela Corte Constitucional.

Por ocasião do **Tema de Repercussão Geral nº 225**, em 2016, relativo ao Recurso Extraordinário nº 601.314, no qual foi discutida a constitucionalidade do artigo 6º,

da Lei Complementar nº 105/2001¹⁵ frente à garantia do sigilo bancário, o STF chancelou a possibilidade de fornecimento de informações bancárias sigilosas **diretamente ao FISCO sem a necessidade de autorização judicial desde que** atendidos os **requisitos objetivos** e mediante a **transferência da responsabilidade** de guarda e manutenção do sigilo das informações bancárias para a esfera fiscal, ao que nomeou como ***transferência das esferas de sigilo bancário para o fiscal:***

Tema nº 225:

CONSTITUCIONAL. SIGILO BANCÁRIO. FORNECIMENTO DE INFORMAÇÕES SOBRE MOVIMENTAÇÃO BANCÁRIA DE CONTRIBUINTES, PELAS INSTITUIÇÕES FINANCEIRAS, DIRETAMENTE AO FISCO, SEM PRÉVIA AUTORIZAÇÃO JUDICIAL (LEI COMPLEMENTAR 105/2001). POSSIBILIDADE DE APLICAÇÃO DA LEI 10.174/2001 PARA APURAÇÃO DE CRÉDITOS TRIBUTÁRIOS REFERENTES A EXERCÍCIOS ANTERIORES AO DE SUA VIGÊNCIA. RELEVÂNCIA JURÍDICA DA QUESTÃO CONSTITUCIONAL. EXISTÊNCIA DE REPERCUSSÃO GERAL.

Recurso Extraordinário nº 601.314:

RECURSO EXTRAORDINÁRIO. REPERCUSSÃO GERAL. DIREITO TRIBUTÁRIO. DIREITO AO SIGILO

¹⁵ Art. 6º As autoridades e os agentes fiscais tributários da União, dos Estados, do Distrito Federal e dos Municípios somente poderão examinar documentos, livros e registros de instituições financeiras, inclusive os referentes a contas de depósitos e aplicações financeiras, quando houver processo administrativo instaurado ou procedimento fiscal em curso e tais exames sejam considerados indispensáveis pela autoridade administrativa competente.

(Regulamento)

Parágrafo único. O resultado dos exames, as informações e os documentos a que se refere este artigo serão conservados em sigilo, observada a legislação tributária.

BANCÁRIO. DEVER DE PAGAR IMPOSTOS. REQUISIÇÃO DE INFORMAÇÃO DA RECEITA FEDERAL ÀS INSTITUIÇÕES FINANCEIRAS. ART. 6º DA LEI COMPLEMENTAR 105/01. MECANISMOS FISCALIZATÓRIOS. APURAÇÃO DE CRÉDITOS RELATIVOS A TRIBUTOS DISTINTOS DA CPMF. PRINCÍPIO DA IRRETROATIVIDADE DA NORMA TRIBUTÁRIA. LEI 10.174/01.

1. O litígio constitucional posto se traduz em um confronto entre o direito ao sigilo bancário e o dever de pagar tributos, ambos referidos a um mesmo cidadão e de caráter constituinte no que se refere à comunidade política, à luz da finalidade precípua da tributação de realizar a igualdade em seu duplo compromisso, a autonomia individual e o autogoverno coletivo.

2. Do ponto de vista da autonomia individual, o sigilo bancário é uma das expressões do direito de personalidade que se traduz em ter suas atividades e informações bancárias livres de ingerências ou ofensas, qualificadas como arbitrárias ou ilegais, de quem quer que seja, inclusive do Estado ou da própria instituição financeira.

3. Entende-se que a igualdade é satisfeita no plano do autogoverno coletivo por meio do pagamento de tributos, na medida da capacidade contributiva do contribuinte, por sua vez vinculado a um Estado soberano comprometido com a satisfação das necessidades coletivas de seu Povo.

4. Verifica-se que o Poder Legislativo não desbordou dos parâmetros constitucionais, ao exercer sua relativa liberdade de conformação da ordem jurídica, na medida em que estabeleceu requisitos objetivos para a requisição de informação pela Administração Tributária às instituições financeiras, assim como manteve o sigilo dos dados a respeito das transações financeiras do contribuinte, observando-se um translado do dever de sigilo da esfera bancária para a fiscal.

5. A alteração na ordem jurídica promovida pela Lei 10.174/01 não atrai a aplicação do princípio da irretroatividade das leis tributárias, uma vez que aquela se encerra na atribuição de competência administrativa à Secretaria da Receita Federal, o que evidencia o caráter instrumental da norma em questão. Aplica-se, portanto, o artigo 144, §1º, do Código Tributário Nacional.

6. Fixação de tese em relação ao item “a” do Tema 225 da sistemática da repercussão geral: “O art. 6º da Lei Complementar 105/01 não ofende o direito ao sigilo bancário, pois realiza a igualdade em relação aos cidadãos, por meio do princípio da capacidade contributiva, bem como estabelece requisitos objetivos e o traslado do dever de sigilo da esfera bancária para a fiscal”.

(...)

8. Recurso extraordinário a que se nega provimento. (RE 601314, Relator(a): Min. EDSON FACHIN, Tribunal Pleno, julgado em 24/02/2016, ACÓRDÃO ELETRÔNICO REPERCUSSÃO GERAL - MÉRITO DJe-198 DIVULG 15-09-2016 PUBLIC 16-09-2016)

A delicadeza relativa à questão do sigilo é perceptível na redação do voto vencedor, elaborado pelo Ministro Edson Fachin, no qual são registrados critérios importantes a serem seguidos para que não se incorra em hipótese de responsabilização decorrente de violação ao sigilo bancário:

Voto Vencedor – Relator Ministro Edson Fachin:

(...)

Nesses termos, a identificação do patrimônio, rendimentos e atividades econômicas do contribuinte pela Administração Tributária serve para a efetivação do princípio da capacidade contributiva, o qual, por sua vez, encontra-se em risco de violação em todas as restritivas hipóteses autorizadas de acesso da Administração Tributária às

transações bancárias dos contribuintes, tal como arroladas nos incisos do art. 3º do Decreto 3.724/01, que regulamenta o art. 6º da lei impugnada. No campo da autonomia individual, verifica-se que o Poder Legislativo não desbordou dos parâmetros constitucionais, ao exercer sua relativa liberdade de conformação da ordem jurídica, na medida em que estabeleceu requisitos objetivos para a requisição de informação pela Administração Tributária às instituições financeiras, assim como manteve o sigilo dos dados a respeito das transações financeiras do contribuinte, observando-se um traslado do dever de sigilo da esfera bancária para a fiscal. Veja-se que o artigo 6º da Lei Complementar 105/01 é taxativo ao facultar o exame de documentos, livros e registros de instituições financeiras, somente se (i) houver processo administrativo instaurado ou procedimento fiscal em curso e (ii) tais exames sejam considerados indispensáveis pela autoridade administrativa competente.

(...)

O acesso às informações fiscais pelas Fazendas Públicas é ferramenta indispensável de garantia da própria sistemática republicana, prática legitimada pela Corte Guardiã da Constituição. Ainda assim, para que não se incorra em violação ao sigilo fiscal, mesmo as Fazendas Públicas devem observar e seguir os requisitos objetivos chancelados pelo Supremo Tribunal Federal.

Na mesma linha, posteriormente, em dezembro de 2019, o **Tema da Repercussão Geral nº 990**, *leading case* **Recurso Extraordinário 1.055.941**, enfrentou questão relativa à possibilidade do compartilhamento de dados bancários e fiscais, naturalmente sigilosos, obtidos pela Receita Federal no legítimo exercício de seu

dever de fiscalizar, **diretamente ao Ministério Público, para fins penais, sem autorização prévia do Poder Judiciário**, à luz dos arts. 5º, incs. X e XII, 145, § 1º, e 129, inc. VI, da Constituição da República. Por maioria, o Tribunal aderiu à proposta formulada pelo Ministro Alexandre de Moraes e deram provimento ao recurso, firmando a seguinte tese de repercussão geral:

Tese 990

Possibilidade de compartilhamento com o Ministério Público, para fins penais, dos dados bancários e fiscais do contribuinte, obtidos pela Receita Federal no legítimo exercício de seu dever de fiscalizar, sem autorização prévia do Poder Judiciário.

Nessa oportunidade, o acesso de informações sigilosas pelo Ministério Público sem a necessidade de autorização judicial foi reconhecido. **Porém, assim como no caso das Fazendas Públicas, não deve se dar indiscriminadamente**, mas mediante o enquadramento da necessidade ou justificativa em alguma das hipóteses legais ou requisitos mencionados pelo *decisum*:

Decisão: O Tribunal, por maioria, aderindo à proposta formulada pelo Ministro Alexandre de Moraes, fixou a seguinte tese de repercussão geral:

“1. É constitucional o compartilhamento dos relatórios de inteligência financeira da UIF e da íntegra do procedimento fiscalizatório da Receita Federal do Brasil, que define o lançamento do tributo, com os órgãos de persecução penal para fins criminais, sem a obrigatoriedade de prévia autorização judicial, devendo ser resguardado o sigilo das informações em procedimentos formalmente instaurados e sujeitos a posterior controle jurisdicional.

2. O compartilhamento pela UIF e pela RFB, referente ao item anterior, deve ser feito unicamente por meio de comunicações formais, com garantia de sigilo, certificação

do destinatário e estabelecimento de instrumentos efetivos de apuração e correção de eventuais desvios.”, vencido o Ministro Marco Aurélio, que não referendava a tese. Presidência do Ministro Dias Toffoli. Plenário, 04.12.2019.

Destarte, como decidido pelo Plenário do Supremo Tribunal Federal, o fornecimento de informações fiscais e financeiras amparadas pelo sigilo diretamente a **órgãos de persecução penal para fins criminais** é legítimo e prescindirá de autorização judicial **DESDE QUE** respeitadas os seguintes limites:

- (i) as informações sejam transmitidas **exclusivamente** por meio de **comunicações formais**;
- (ii) exista **garantia da manutenção do sigilo**;
- (iii) haja **certificação do destinatário**;
- (iv) sejam estabelecidos **instrumentos efetivos de apuração e correção** de eventuais desvios;

A interpretação sistemática desses dois temas de repercussão geral torna patente a preocupação da Corte Constitucional com a preservação da privacidade e do sigilo dos dados, bem como a necessidade da **existência de caso concreto de contribuinte**¹⁶ cujos dados precisem ser conhecidos pelo Ministério Público para fins de **persecução**

¹⁶ Ou situação específica, cujos contribuintes sejam *anonimizados*, bem como bem delimitada a situação, tal qual descrito na Manifestação Técnica PG/PADM/T/008/PRSM, aprovada pela Chefia e Subprocuradora Geral Consultiva, cujas respostas me parece – e me penitencio pela subtração ao visto de então – devam estar cercadas das mesmas cautelas que permitam a identificação do procedimento através do qual estejam sendo demandadas, dos agentes que tenham acesso aos dados, da motivação para a demanda, bem como do rastreamento de eventuais desvios.

penal, devidamente documentado em comunicação formal.

O sopesamento entre os bens jurídicos ***privacidade ↔ principio redistributivo do tributo*** (mediante combate a fraudes e desvios que subtraem da base de cálculo da tributação significativos valores de contribuintes que pretendem se beneficiar da própria torpeza) deve chegar num ponto ótimo em que cada um sofra o menor dano possível, funcionando como “mandados de otimização”¹⁷, de modo a resguardar a própria sistemática constitucional democrática.

Nessa toada, a solução de equilíbrio e coexistência de ambos os bens jurídicos fornecida nas decisões de controle de constitucionalidade envolvendo sigilo fiscal estaria na **restrição da transferência de acesso às informações sigilosas às hipóteses legais ou realmente necessárias, justificáveis e concretas, bem como no controle do caminho percorrido pelas informações.** Isso é evidenciado também pelas expressões escolhidas para sintetizar as exigências: “comunicações formais”, “certificação do destinatário”, “garantia da manutenção do sigilo” e “instrumentos efetivos de apuração e correção de eventuais desvios”.

Essa logística visa permitir a identificação e responsabilização administrativa, civil e criminal do agente público que venha a fazer uso indevido da informação sigilosa à qual teve acesso em razão da função. Assim, a necessidade identificação de quem acessa tais informações é algo simplesmente elementar para o cumprimento da lei, a fim de que

aqueles valores constitucionais como privacidade e personalidade do indivíduo sejam preservados pelo Estado.

Impende registrar que a ementa do *leading case* Recurso Extraordinário 1.055.941, se encontra disponível no Portal do Supremo, porém o acórdão ainda não foi publicado nem disponibilizado no Portal do STF, não sendo possível ter acesso à integralidade do conteúdo decisório na presente data, inviabilizando a análise das motivações do *decisum*. Não obstante isso, a clareza dos elementos acima esmiuçados nos permitiu desde logo o prolatar da presente análise.

No ponto, ao caso em tela não parecem ser aplicáveis os exatos termos do enunciado relativo ao Tema 990, da Repercussão Geral.

No caso, não se trata de solicitação de acesso a dados pertencentes a indivíduo específico, porquanto o que se pretende é o acesso a banco de dados de forma generalizada.

Sequer é possível mensurar a quantidade de cidadãos afetados pelo pretendido acesso. **Nessa linha, não é possível presumir a existência de motivação compatível com instrução criminal ou motivação fiscalizatória específica que recaia sobre a totalidade dos indivíduos cadastrados no banco de dados cujo acesso se pretende obter, em que pesem as nobilíssimas funções de controle externo do Egrégio Tribunal de Contas deste Município.**

Isto é, se possível fosse o fornecimento de acesso automático a tal banco de dados pela ilustre Corte de Contas, estaria a Fazenda Pública a lha conferir mais prerrogativas do que goza o próprio Ministério Público,

¹⁷ ALEXY, Robert. **Derecho e razón práctica**. México: Fontamara, 1993, p.87, n. 27

viabilizando o acesso a informações sigilosas sem a demonstração de atendimento a nenhum dos critérios, quer legais, quer chancelados pela Corte Constitucional.

A agravar o quadro de vulnerabilidade do contribuinte, de cujas informações sigilosas a Fazenda fiel depositária, **é incalculável o quantitativo de informações que estão disponíveis em tal banco de dados.** A qualidade e especificidade das informações nele cadastradas também não é informada. Outrossim, não há evidência que demonstre a **necessidade e a finalidade pública** que se pretende alcançar pela liberação de acesso tão amplo.

Cumpra lembrar, a este propósito, que é justamente a necessidade dos **dados sigilosos para fins de instrução fiscalizatória ou criminal** o argumento capaz de afastar as vedações relativas ao sigilo fiscal e viabilizar o acesso a informações protegidas fora daquelas legalmente previstas no artigo 198 do Código Tributário Nacional.

O reiterado posicionamento do Supremo Tribunal Federal sobre o tema, mantendo a necessidade do enquadramento legal e preenchimento de requisitos específicos mesmo nas circunstâncias em que o acesso a tais dados se mostra essencial, torna cristalino **que o acesso aos dados sigilosos não é, nem pode ser, um fim em si mesmo** a viabilizar às instituições o acesso indiscriminado por seus respectivos agentes a dados de qualquer cidadão sem motivação, sendo certo que para ser legítimo e assim não atrair a responsabilização, **o acesso a informações sigilosas deve ser individualizado, fundamentado e rastreável.**

Isto posto, é imprescindível a **delimitação de forma objetiva**, pelo setor técnico responsável, acerca de **quais informações** se encontram disponíveis no banco de dados cujo acesso se pretende, assim como o requerimento de acesso às informações deve ser **fundamentado. Outrossim, deve ser informado: (i) se há possibilidade de escolher quais informações serão acessadas pelo requerente; (ii) se há possibilidade de identificar o agente responsável pelo acesso de cada informação e certificar seu acesso; (iii) se o acesso a informações de tal banco de dados eletrônico não põe em risco a manutenção do sigilo em relação aos dados não fornecidos ou acesso por terceiros não autorizados; e (iv) quais os mecanismos de controle disponíveis para auditar os acessos.**

Mas não é só.

Por outro lado, há de se ter em vista que o requerente *in casu* não é o Ministério Público, mas o Tribunal de Contas do Município do Rio de Janeiro – TCMRJ, órgão de fiscalização e controle externo auxiliar do Poder Legislativo Municipal, instituições detentoras de jurisdição e atribuições diversas e que recentemente o Supremo Tribunal Federal negou compartilhamento de informações de operadoras de telefonia celular com o IBGE em virtude da vagueza das razões pelas quais foram reclamadas, conforme explicitado na Parte I desta Manifestação.

Dispõe o § 1º, do artigo 31, da Constituição Federal:

Art. 31. A fiscalização do Município será exercida pelo Poder Legislativo Municipal, mediante controle externo, e pelos sistemas de controle interno do Poder Executivo Municipal, na forma da lei.

§ 1º O controle externo da Câmara Municipal será exercido com o auxílio dos Tribunais de Contas dos Estados ou do Município ou dos Conselhos ou Tribunais de Contas dos Municípios, onde houver. (g.n.)

Os artigos 88 e 95 da Lei Orgânica do Município do Rio de Janeiro elencam as atribuições do TCMRJ:

Art. 88 - O controle externo, a cargo da Câmara Municipal, será exercido com o auxílio do Tribunal de Contas do Município, ao qual compete:

I - apreciar as contas prestadas anualmente pelo Prefeito, mediante parecer prévio que deverá ser elaborado em sessenta dias a contar de seu recebimento;

II - julgar as contas dos administradores e demais responsáveis por dinheiros, bens e valores públicos da administração direta, indireta e fundacional e sociedades constituídas e mantidas pelo Poder Público, e as contas daqueles que derem causa a perda, extravio ou outra irregularidade de que resulte prejuízo ao erário;

III - apreciar, para fins de registro, a legalidade:

a) dos atos de admissão de pessoal, a qualquer título, na administração direta, indireta e fundacional, excetuadas as nomeações para cargo de provimento em comissão;

b) das concessões de aposentadorias e pensões, ressalvadas as melhorias posteriores que não alterem o fundamento legal do ato concessório;

IV - realizar, por iniciativa própria, da Câmara Municipal, de comissão técnica ou de inquérito, inspeções e auditorias de natureza contábil, financeira, orçamentária, operacional e patrimonial nas unidades administrativas dos Poderes Legislativo e Executivo e demais entidades referidas no inciso II;

V - acompanhar as contas de empresas estaduais ou federais de que o Município

participe, de forma direta ou indireta, nos termos do respectivo estatuto;

VII - fiscalizar a aplicação de quaisquer recursos transferidos ao Município ou por ele repassados mediante convênio, acordo, ajuste ou outro instrumento a instituições públicas e privadas de qualquer natureza;

VII - fiscalizar a execução de convênios, acordos, ajustes ou outros instrumentos congêneres com a União e o Estado para a aplicação de programas comuns;

VIII - prestar as informações solicitadas pela Câmara Municipal ou por qualquer de suas Comissões sobre a fiscalização contábil, financeira, orçamentária, operacional e patrimonial e sobre resultados de auditorias e inspeções realizadas;

IX - aplicar aos responsáveis, em caso de ilegalidade de despesa ou irregularidade de contas, as sanções previstas em lei, incluindo, entre outras cominações, multa proporcional ao dano causado ao erário;

X - assinar prazo para que o órgão ou entidade adote as providências necessárias ao exato cumprimento da lei, se verificada ilegalidade;

XI - sustar, se não atendido, a execução do ato impugnado, comunicando a decisão à Câmara Municipal;

XII - representar ao Poder competente sobre irregularidades ou abusos apurados;

XIII - manter cadastro e arquivo dos contratos de obras, serviços e compras firmados pelos órgãos municipais e dos laudos e relatórios de aceitação definitiva ou provisória de obras por eles realizadas.

(...)

Art. 95 - Além das atribuições definidas no art. 88, compete ao Tribunal de Contas:

I - eleger seus órgãos diretivos;

II - elaborar seu regimento interno, com observância das normas de processo e das garantias processuais das partes, dispondo sobre a competência e o funcionamento de seus órgãos internos;

III - organizar suas secretarias e serviços auxiliares, zelando pelo exercício da atividade correcional;

IV - propor à Câmara Municipal projetos de lei sobre organização, funcionamento, polícia, criação, transformação ou extinção dos cargos, empregos e funções de seus serviços e fixação da respectiva remuneração, observados os parâmetros estabelecidos na lei de diretrizes orçamentárias;

V - conceder licença, férias, aposentadoria e outros afastamentos a servidores que lhe forem imediatamente vinculados;

VI - prover, por concurso público de provas ou de provas e títulos, os cargos de seus serviços auxiliares, excetuados os de confiança assim definidos em lei. (g.n.)

Não há dúvidas de que, na forma da LGPD, de que se tratou na Parte II deste pronunciamento, a Egrégia Corte de Contas desfruta de atribuição legal para o compartilhamento de dados com o Município do Rio de Janeiro, no exercício do controle externo, mas o exerce de forma adequada, finalística e motivada.

Nessa toada, a solicitação de acesso a informações sigilosas de forma tão ampla, sem menção ao escopo do exercício *in concreto* de suas competências de controle externo, me parece **ultrapassar os próprios interesses institucionais do Tribunal de Contas do Município**, tornando injustificada e desbordando dos limites legais a disponibilização de informações com tal amplitude. Frise-se: nem mesmo ao Ministério Público foi dado tal *cheque em branco*.

Registre-se, porém, que **não se trata de impossibilidade absoluta de acesso a informações protegidas pelo sigilo fiscal diretamente ao nobre Tribunal de Contas,**

mas da necessidade de, uma vez que não incorra em nenhuma das hipóteses legais do artigo 198, do Código Tributário Nacional, seja demonstrado o **preenchimento dos requisitos enumerados pelo Supremo Tribunal Federal**, assim como aqueles enumerados pela LGPD e já arrolados.

Conforme identificado na Manifestação Técnica PG/PADM/T/008/2020/PRSM, aprovada pela PG/SUBCONS, o compartilhamento de dados anonimizados sobre os quais caiba fiscalização pelo Tribunal de Contas atende aos princípios da transparência da Administração Pública, que, lado outro, não deve ser infensa a controle; antes, o contrário.

Por sua vez, o STF, através das ementas a seguir, esclarece que, para os Tribunais de Contas, o acesso a informações sigilosas, sob este prisma, não é mais fácil ou simples do que para o Ministério Público, restringindo- o a informações relativas à fiscalização e destinação de verbas públicas e afastando-o nos casos que fujam ao escopo institucional ou digam respeito a informações individuais e pessoais:

EMENTA AGRAVO INTERNO EM MANDADO DE SEGURANÇA. DELIBERAÇÕES DO TRIBUNAL DE CONTAS DA UNIÃO QUE DETERMINARAM O FORNECIMENTO DE TRABALHOS DE AUDITORIA INTERNA. RECUSA DE ENTREGA, POR PARTE DO BANCO DO BRASIL S.A., SOB A INVOCAÇÃO DOS SIGILOS BANCÁRIO E EMPRESARIAL. AUSÊNCIA DE LIQUIDEZ E CERTEZA DOS FATOS EM QUE SE FUNDA A IMPETRAÇÃO. **SIGILO BANCÁRIO QUE NÃO SE APLICA A DADOS INERENTES À SOCIEDADE DE ECONOMIA MISTA, ENQUANTO ENTIDADE INTEGRANTE DA ADMINISTRAÇÃO PÚBLICA INDIRETA, NEM A OPERAÇÕES**

QUE ENVOLVAM RECURSOS PÚBLICOS. OCULTAMENTO DE DADOS PESSOAIS E DE MOVIMENTAÇÕES INDIVIDUAIS DE CORRENTISTAS ADMITIDO PELA AUTORIDADE IMPETRADA. INVIABILIDADE DE INVOCAR SIGILO EMPRESARIAL PARA SONEGAR DOCUMENTO REQUISITADO POR ÓRGÃO DE CONTROLE EXTERNO. 1. Quando enfocados apenas dados operacionais da sociedade de economia mista, sem identificação de dados pessoais ou de movimentações individuais dos correntistas, não há falar em sigilo bancário como óbice ao fornecimento dos documentos de auditoria interna requisitados pelo TCU. Esse é o entendimento que se extrai dos princípios da publicidade e da transparência, além da exigência de prestar contas, inerentes, por imposição constitucional (MS 23168 AgR. Órgão julgador: Primeira Turma. Relator(a): Min. ROSA WEBER. Julgamento: 28/06/2019. Publicação: 05/08/2019

Lei nº 8.666/93; art. 1º da Lei nº 9.613/98 e art. 1º, I e II, do DL nº 201/67). Trancamento. Descabimento. Sigilo bancário. Inexistência. Conta corrente de titularidade da municipalidade. Operações financeiras que envolvem recursos públicos. Requisição de dados bancários diretamente pelo Ministério Público. Admissibilidade. Precedentes. Extensão aos registros de operações bancárias realizadas por particulares, a partir das verbas públicas creditadas naquela conta. Princípio da publicidade (art. 37, caput, CF). Prova lícita. Recurso não provido.

1. Como decidido pelo Supremo Tribunal Federal, ao tratar de requisição, pelo Tribunal de Contas da União, de registros de operações financeiras, “o sigilo de informações necessárias para a preservação da intimidade é relativizado quando se está diante do interesse da sociedade de se conhecer o destino dos

recursos públicos” (MS nº 33.340/DF, Primeira Turma, Relator o Ministro Luiz Fux, DJe de 3/8/15). 2. Assentou-se nesse juízo que as “operações financeiras que envolvam recursos públicos não estão abrangidas pelo sigilo bancário a que alude a Lei Complementar nº 105/2001, visto que as operações dessa espécie estão submetidas aos princípios da Administração Pública insculpidos no art. 37, caput, da Constituição. (...)

(RHC 133118. Órgão julgador: Segunda Turma. Relator(a): Min. DIAS TOFFOLI. Julgamento: 26/09/2017. Publicação: 09/03/2018)

Destarte, existem informações protegidas pelo sigilo fiscal que podem ser diretamente fornecidas aos Tribunais de Contas, porém, é necessário que tal análise se dê de forma específica: seja porque individualizada, não apenas em razão dos requisitos fixados pelo Supremo Tribunal Federal nos Temas de Repercussão Geral nº 225 e nº 990, mas para que seja possível identificar se a necessidade de acesso a informação determinada está relacionada ao exercício do seu dever institucional, seja porque individualizável, qual seja, quando a informação que se pretende obter diz respeito a uma determinada “verba”, que seja objeto de fiscalização pela Corte de Contas, hipótese em que, uma vez *desidentificados* ou *anonimizados* os contribuintes, os dados, neste caso, poderão ser fornecidos de forma não individualizada.

Nesta toada, a título de ilustração, vale a menção de que o Governo Federal editou o Decreto Federal n. 10.209, de 22 de janeiro de 2020, permitindo que a Controladoria-Geral da União e o Tribunal de Contas da União tenham acesso a dados de órgãos do Ministério da Economia, inclusive da Receita

Federal, com sigilo fiscal. A permissão de compartilhamento, todavia, não se aplica: (i) a dados decorrentes de transferência de sigilo bancário à administração tributária ou (ii) econômico-fiscais provenientes de acordo de cooperação internacional no qual tenha sido vedada a transferência dos dados a órgãos externos à administração tributária e aduaneira, bem como (c) "**de dados genéricos, desproporcionais, imotivados ou desvinculados dos procedimentos de auditoria ou inspeção**", exatamente na linha hermenêutica que aqui se preconiza, (d) de **informações protegidas por sigilo fiscal** ou por sigilo profissional ou (e) o repasse das informações a terceiros.

Vale ressaltar, por fim, neste caso, a título de mera ilustração, que o Conselho Federal da Ordem dos Advogados do Brasil, em caso análogo, ajuizou, perante o Supremo Tribunal Federal, a Ação Direta de Inconstitucionalidade n. 6649 em face do Decreto Federal n. 10.046/2019 da Presidência da República, *que dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados*, justamente por se tratar de uma ferramenta de vigilância estatal, que inclui informações pessoais, familiares e trabalhistas básicas de todos os brasileiros, mas também de dados pessoais sensíveis, como dados biométricos, que podem ser coletados para reconhecimento automatizado, como a palma da mão, as digitais, a retina ou a íris, o formato da face, a voz e a maneira de andar, que viola os direitos fundamentais à privacidade, à proteção de dados pessoais e à *autodeterminação informativa*.

A ação veio a ser distribuída, por prevenção, ao Ministro Gilmar Mendes, em razão da Arguição de Descumprimento de Preceito Fundamental (ADPF) 695, com pedido de suspensão do compartilhamento de dados dos mais de 76 milhões de brasileiros que possuem Carteira Nacional de Habilitação (CNH) pelo Serviço Federal de Processamento de Dados (Serpro) com a Agência Brasileira de Inteligência (Abin), cuja Medida Cautelar fora indeferida em 24/06/2020, antes da decisão plenária que acolheu o voto da Ministra Rosa Weber no *case* paradigmático da impossibilidade de compartilhamento de dados entre pessoa jurídica de direito público e privado, menos por esta circunstância, do que pelos mesmos direitos fundamentais apontados nas ações conexas acima reunidas por prevenção.

O tema, portanto, ainda promete novos debates no âmbito do Supremo Tribunal Federal, no campo do compartilhamento genérico de dados, porém, porquanto já se tenha dele tratado, sem necessariamente essa nomenclatura, em matéria de compartilhamento de dados cobertos por sigilo fiscal, como no caso em apreço, os quais merecem tratamento especial, espera-se que a Corte e os *amicus curiae* admitidos ao debate se lembrem disso.

III - CONCLUSÃO

As informações não individualizáveis e informações de natureza pública não estão sujeitas à vedação decorrente do sigilo fiscal, devendo no primeiro caso ser garantido sempre o anonimato. Nos termos da Manifestação Técnica PG/PADM/T/008/2020/PRSM, também é possível a criação de códigos (ou inscrições)

correspondentes às inscrições fiscais ou imobiliárias como solução a viabilizar o fornecimento desidentificado de informações sigilosas, com as cautelas de estilo.

No que tange ao fornecimento automático (sem a necessidade de autorização judicial) de informações protegidas pelo sigilo fiscal pelo Tribunal de Contas do Município, o mesmo será possível desde que demonstrado o atendimento integral dos requisitos fixados na Lei Geral de Proteção de Dados, no art. 198 do Código Tributário Nacional e dos construídos pela jurisprudência do Supremo Tribunal Federal, atraindo a análise individualizada.

Por fim, resta consignar que, diante da ausência de previsão legal específica e das condicionantes levantadas pela jurisprudência, ressalvada a possibilidade de ser demonstrado que todos os requisitos restaram atendidos, é atraída a análise individualizada, afastando a possibilidade de acesso automático a **todas** as informações.

É o que me parece e que submeto à douta apreciação da ilustrada Chefia desta Procuradoria Administrativa, haja vista o ineditismo da matéria.

ARÍCIA FERNANDES CORREIA

Procuradora do Município do Rio de Janeiro

Matr: 11/152.446-1 – OAB/RJ 79.271

Visto PG/PADM/097/2021/CR

Manifestação Técnica

PG/PADM/T/025/2021/AFC

Análise da possibilidade de acesso ao SIF pelos auditores do TCM frente às disposições da LGPD

Trata-se de consulta jurídica encaminhada pelo Subsecretário de Tributação e Fiscalização questionando a possibilidade de disponibilização de acesso integral ao Sistema de Inteligência Fiscal – SIF pelos auditores do Tribunal de Contas do Município, a ser realizada pela Secretaria Municipal de Fazenda e Planejamento, face a previsão do art. 198 do Código Tributário Nacional e diante do assento constitucional do *sigilo fiscal* e da *autodeterminação informacional* que vigoram no ordenamento jurídico pátrio.

É sabido que, apesar de não ter contornos rígidos de aplicação ainda definidos em nenhuma *quaestio*, a LGPD tutela inúmeros direitos, seja de pessoas físicas ou jurídicas, no meio digital ou não. Também é cediço que todo e qualquer dado merece proteção constitucional, e que ao compartilhá-los, é exigido ônus justificativo.

Nos termos da lei em comento, o MRJ figura como *controlador* de informações sigilosas e sensíveis. Nessa condição, para que válidos e lícitos, o tratamento e o compartilhamento de dados deverão atender às bases legais e jurisprudenciais já elencadas na manifestação aqui vistada, além dos princípios e as diretrizes desta casa jurídica igualmente apontados.

Ante ao exposto, aprovo a bem lançada **Manifestação Técnica PG/PADM/T/025/2021/AFC**, por suas próprias razões e fundamentos, visto ter a explanação de fls. 06/41 trilhado de forma

exaustiva as balizas a serem adotadas, por ora, na consulta formulada.

Cumpra pontuar que, conforme mencionado pela i. Procuradora Arícia Fernandes Correa, a advocacia pública encontra atualmente grande desafio ao orientar os órgãos que assiste, tendo em vista a existência de políticas públicas conjuntas que compartilham dados, além de ser um debate nascente e dotado de diversas divergências doutrinárias.

À SMFP.

Rio de Janeiro, 29 de abril de 2021.

CARLOS RAPOSO
Procurador-Chefe da Procuradoria
Administrativa
Mat. 11/221.206.6 - 113.571 - OAB/RJ