



UNIVERSIDADE DE BRASÍLIA
FACULDADE DE DIREITO
PROGRAMA DE PÓS-GRADUAÇÃO EM DIREITO

JOÃO GABRIEL COSTA DOS SANTOS

**Tributação movida a dados: standards para a coleta e a transferência de
informações pelo Fisco brasileiro**

Brasília – DF
2023

JOÃO GABRIEL COSTA DOS SANTOS

**Tributação movida a dados: standards para a coleta e a transferência de
informações pelo Fisco brasileiro**

***Data-driven taxation: standards for the collection and transfer of information
by Brazilian tax authorities***

Dissertação apresentada ao Programa de Pós-Graduação em Direito da Universidade de Brasília como requisito parcial para a obtenção do título de Mestre em Direito.

Orientador: Prof. Dr. Antônio de Moura Borges.

Brasília – DF

2023

Ficha catalográfica elaborada automaticamente,
com os dados fornecidos pelo(a) autor(a)

SS237t Santos, João Gabriel Costa dos
Tributação movida a dados: standards para a coleta e a
transferência de informações pelo Fisco brasileiro / João
Gabriel Costa dos Santos; orientador Antônio de Moura
Borges. -- Brasília, 2023.
152 p.

Dissertação(Mestrado em Direito) -- Universidade de
Brasília, 2023.

1. Direito Tributário. 2. Proteção de Dados. 3. Sigilo
Fiscal. 4. Direito à Privacidade. 5. Tratamento de Dados. I.
Borges, Antônio de Moura, orient. II. Título.

JOÃO GABRIEL COSTA DOS SANTOS

Tributação movida a dados: standards para a coleta e a transferência de informações pelo Fisco brasileiro.

Dissertação apresentada ao Programa de Pós-Graduação em Direito da Universidade de Brasília como requisito parcial para a obtenção do título de Mestre em Direito.

Aprovada em 17 de outubro de 2023.

BANCA EXAMINADORA:

Professor Doutor Antônio de Moura Borges (Orientador)
Universidade de Brasília (UnB)

Professor Doutor Gilmar Ferreira Mendes
Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa (IDP)

Professora Doutora Cristiane de Oliveira Coelho Galvão
Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa (IDP)

Professora Doutora Debora Bonat (Suplente)
Universidade de Brasília (UnB)

Este trabalho é dedicado a todos que lutam em defesa das instituições democráticas.

AGRADECIMENTOS

Como nada se conquista sozinho, esta dissertação é a junção de vivências que, felizmente, tive com amigos, familiares, professores e colegas de profissão e de academia. Sou grato a cada um que tomou seu tempo para me apoiar nessa jornada, cada qual à sua forma, com a sua contribuição, mas todos essenciais para que este trabalho pudesse se concretizar.

Agradeço ao Professor Antônio de Moura Borges, nosso decano, pelas valiosas lições no decorrer da sua orientação. Foi uma troca memorável e muito enriquecedora.

Ao Professor Gilmar Ferreira Mendes, por me oportunizar experiências inestimáveis de crescimento pessoal, acadêmico e profissional e por tudo que me ensinou. Também remeto os agradecimentos à competente equipe do seu gabinete, que me inspira diariamente: Ana Carvalhal, Andréa Gonzaga, Anna Finageiv, Beatriz Horbach, Berenice Leite, Carla Zottmann, Carlos Eduardo, Diego Veras, Eduardo Granzotto, Jaizinho Rodrigues, Jean Minuzzi, Joecio Lima, Lucas Faber, Marcelo Kreimer, Marcus Bastos, Maria Viotti, Monique Siqueira, Renata Braz, Rômulo Gobbi, Suely Camargo, Tarsila Fernandes.

À Professora Cristiane Coelho Galvão, que lançou as luzes para o meu objeto de pesquisa ainda na fase inicial. Nossas conversas foram fundamentais para o nascimento deste projeto.

À Professora Debora Bonat e ao Professor Fabiano Hartmann, por me proporcionarem uma oportunidade única de aprendizado no Laboratório e Grupo de Pesquisa Direito, Racionalidade e Inteligência Artificial (DR.IA), da Universidade de Brasília (UnB).

Aos queridos amigos de escola, de UnB, de profissão, de vida, que sempre me apoiam e me dão a certeza (e a segurança) de que não caminho sozinho. Em especial, menciono aqueles que foram imprescindíveis para que esta dissertação ganhasse forma: Alberto Medeiros, Alexandre Morais, Gabriel Fonseca, Gabriel Freitas, Guilherme Lacerda, Gustavo Lima, João Fidanza, Matheus Pimenta, Paulo Sávio, Pedro Aurélio, Pedro Burached, Renan Carvalho, Valter Vitelli e Victor Oliveira.

À minha família, meu “imenso desmedido amor”; notadamente aos meus avós (em memória), Antônio Santos, Armando Bayma, Maria Santos e Nazilde Costa; aos

meus pais, Josias Santos e Silvia Costa; à minha irmã, Mariah Santos; aos meus tios Carlos Moura, Lindalva Monteiro e Silvana Costa; e aos meus primos Eduardo Pomponio, Fernanda Costa, Lucas Oliveira e João Paulo Oliveira.

Por fim, agradeço a todos os professores e demais profissionais da Universidade de Brasília que me auxiliaram durante os meses de pesquisa e tornaram este processo muito mais prazeroso. Uma das maiores felicidades desta experiência foi poder retornar à minha querida UnB.

*“Caminhante, são tuas pegadas, o
caminho e nada mais;
Caminhante, não há caminho, faz-se
caminho ao andar.”
(Antonio Machado)*

RESUMO

Com as transformações ocorridas na Era da Informação, os novos paradigmas tecnológicos impactaram não apenas a esfera privada, mas também as ações desempenhadas pelo setor público. Por conseguinte, tem-se observado uma crescente utilização de bancos de dados para o incremento de políticas e serviços estatais, a exemplo das mudanças verificadas na dinâmica da atividade tributária, que passou a demandar um constante fluxo de informações dos sujeitos passivos para ser exercida. Esta dissertação de mestrado visa investigar, à luz dos direitos à privacidade e à proteção de dados, as balizas para a operação de tratamento de dados pessoais realizada pelas autoridades brasileiras nos processos de fiscalização e de cobrança de tributos. Com isso, objetiva-se estabelecer os parâmetros para a atuação do Fisco nas plataformas digitais, com base nos critérios de proteção de dados definidos no ordenamento jurídico brasileiro e nas diretrizes internacionais. Dessa forma, são analisados os conceitos relativos às garantias individuais dos contribuintes e as regras vigentes acerca do uso de informações fiscais. Discorre-se sobre a redefinição do direito à privacidade a partir da noção de autodeterminação informativa, bem assim acerca da evolução do conceito de sigilo fiscal. Em seguida, são examinadas as normas internas em relação ao tema, com enfoque no processo de coleta de informações realizado pela Secretaria Especial da Receita Federal do Brasil (RFB). Posteriormente, são descritas as regras previstas na Lei Geral de Proteção de Dados (LGPD) para, assim, definir seu alcance no campo da troca de informações tributárias. Por fim, são abordados os *standards* para a atuação da Administração Tributária na economia movida a dados, notadamente os limites impostos à coleta e à transmissão de informações e as penalidades aplicáveis aos agentes públicos no âmbito dessas operações. Também são explorados exemplos do direito comparado e normas internacionais sobre o assunto. Com suporte na nova leitura conferida ao direito à privacidade, conclui-se que o argumento da mera preservação do sigilo fiscal é insuficiente para legitimar o uso indiscriminado de dados pessoais de contribuintes no bojo da atividade fiscalizadora da Fazenda Pública.

Palavras-chave: direito tributário; proteção de dados; sigilo fiscal; direito à privacidade; tratamento de dados.

ABSTRACT

With the transformations that have taken place in the Information Age, the new technological paradigms impacted not only the private sphere, but also the actions performed by the public sector. Consequently, there has been an increasing use of databases to improve state policies and services, such as the changes seen in the dynamics of tax activity, which began to demand a constant flow of information from taxpayers in order to be carried out. This master's thesis aims to investigate, based on the rights to privacy and data protection, the guidelines for the processing of personal data carried out by the Brazilian authorities in tax investigation and collection processes. It intends to establish the parameters for the tax authorities' actions on digital platforms, in line with the data protection criteria defined in the Brazilian legal system and international guidelines. Thus, the concepts relating to taxpayers' individual guarantees and the current rules on the use of tax information are analyzed. It discusses the redefinition of the right to privacy based on the notion of informational self-determination, as well as the evolution of the concept of tax secrecy. Then, the internal regulations on the subject are examined, focusing on the information collection process carried out by the Brazilian Federal Revenue Service (RFB). Subsequently, the rules set out in the Brazilian General Data Protection Law (LGPD) are described to define their scope in the field of tax information exchange. Finally, the standards for the Tax Administration's actions in the data-driven economy are addressed, notably the limits imposed on the collection and transfer of information and the penalties applicable to public agents in the context of these operations. Examples from comparative law and international standards on the subject are also explored. Based on the new interpretation of the right to privacy, it is concluded that the argument of the mere preservation of tax secrecy is insufficient to legitimize the indiscriminate use of taxpayers' personal data within the scope of the tax authorities' inspection activities.

Keywords: tax law; data protection; tax secrecy; right to privacy; data processing.

LISTA DE ABREVIATURAS E SIGLAS

ADI	Ação Direta de Inconstitucionalidade
ADPF	Arguição de Descumprimento de Preceito Fundamental
AEoI	<i>Automatic Exchange of Information</i>
AGU	Advocacia-Geral da União
ANPD	Autoridade Nacional de Proteção de Dados
BACEN	Banco Central do Brasil
BDSG	<i>Bundesdatenschutzgesetz</i>
BEPS	<i>Base Erosion and Profit Shifting</i>
BfDI	<i>Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit</i>
BVerfG	<i>Bundesverfassungsgericht</i>
BZSt	<i>Bundeszentralamt für Steuern</i>
CAEPF	Cadastro Atividade Econômica da Pessoa Física
Cafir	Cadastro de Imóveis Rurais
CbC	<i>Country-by-Country Reporting</i>
CBC	Cadastro Base do Cidadão
CCGD	Comitê Central de Governança de Dados
CEDH	Convenção Europeia dos Direitos Humanos
CF	Constituição Federal
CFOAB	Conselho Federal da Ordem dos Advogados do Brasil
CGU	Controladoria-Geral da União
CMN	Conselho Monetário Nacional
CNO	Cadastro Nacional de Obras
CNPJ	Cadastro Nacional da Pessoa Jurídica
Coaf	Conselho de Controle de Atividades Financeiras
Cocad	Coordenação-Geral de Gestão de Cadastros e Benefícios Fiscais
COFINS	Contribuição para o Financiamento da Seguridade Social
CONFAZ	Conselho Nacional de Política Fazendária
CONSIF	Confederação Nacional do Sistema Financeiro
CPC	Custo Por Clique
CPF	Cadastro de Pessoas Físicas
CPMF	Contribuição Provisória sobre Movimentação Financeira

CTN	Código Tributário Nacional
CTSI/RFB	Comitê de Tecnologia e Segurança da Informação da Receita Federal
DDPS	<i>Data-Driven Public Sector</i>
DIMP	Declaração de Informações de Meios de Pagamentos
DOI	Declaração de Operações Imobiliárias
EC	Emenda Constitucional
e-MSF	Manual Eletrônico do Sigilo Fiscal
Eoi	<i>Exchange of Information</i>
EoIR	<i>Exchange of Information on Request</i>
FATCA	<i>Foreign Account Tax Compliance Act</i>
GAFI	Grupo de Ação Financeira
GDPR	<i>General Data Protection Regulation</i>
IBGE	Instituto Brasileiro de Geografia e Estatística
IBS	Imposto sobre Bens e Serviços
ICMS	Imposto sobre Circulação de Mercadorias e Serviços
ICP-Brasil	Infraestrutura de Chaves Públicas Brasileira
INSS	Instituto Nacional do Seguro Social
IOF	Imposto sobre Operações Financeiras
IR	Imposto de Renda
IRS	<i>Internal Revenue Service</i>
IVA	Imposto sobre Valor Agregado
LAI	Lei de Acesso à Informação
LGPD	Lei Geral de Proteção de Dados Pessoais
LIA	Lei de Improbidade Administrativa
MP	Medida Provisória
NCLA	<i>New Civil Liberties Alliance</i>
NF-e	Nota Fiscal Eletrônica
NRA	<i>National Revenue Agency</i>
OCDE	Organização para Cooperação e Desenvolvimento Econômico
PAF	Processo Administrativo Fiscal
PA-RMF	Programa de Atendimento à Requisição de Informações sobre Movimentação Financeira
PEC	Proposta de Emenda à Constituição
PGFN	Procuradoria-Geral da Fazenda Nacional

PIS	Contribuição para o Programa de Integração Social
Portal e-CAC	Portal do Centro Virtual de Atendimento ao Contribuinte
PSB	Partido Socialista Brasileiro
RE	Recurso Extraordinário
RERCT	Regime Especial de Regularização Cambial e Tributária
RFB	Secretaria Especial da Receita Federal do Brasil
RFFP	Representação Fiscal para Fins Penais
RFP	Representação para Fins Penais
RGPD	Regulamento Geral sobre a Proteção de Dados
RIF	Relatório de Inteligência Financeira
RMF	Requisição de Informações sobre Movimentação Financeira
SBR	<i>Standard Business Reporting</i>
Serpro	Serviço Federal de Processamento de Dados
SPB	Sistema de Pagamentos Brasileiro
SPI	Sistema de Pagamentos Instantâneos
STF	Supremo Tribunal Federal
TCU	Tribunal de Contas da União
TEDH	Tribunal Europeu de Direitos Humanos
TIC	Tecnologia da Informação e Comunicação
UE	União Europeia
UIF	Unidade de Inteligência Financeira

SUMÁRIO

INTRODUÇÃO	16
-------------------------	-----------

CAPÍTULO I

AS GARANTIAS CONSTITUCIONAIS DOS CONTRIBUINTES.....	26
1.1 Considerações preliminares	26
1.2 Direito à privacidade	28
1.2.1 Evolução jurisprudencial do STF acerca da correlação da privacidade com a inviolabilidade do sigilo	29
1.2.2 Privacidade como autodeterminação informativa.....	33
1.3 Sigilo Fiscal	35
1.4 Considerações sobre a aplicabilidade do direito à privacidade à luz do sigilo fiscal	47

CAPÍTULO II

O ARCABOUÇO NORMATIVO BRASILEIRO SOBRE A COLETA, TRANSMISSÃO E PROTEÇÃO DE DADOS DOS CONTRIBUINTES.....	51
2.1 Considerações preliminares.....	51
2.2 O processo de coleta e transmissão de informações pelo Fisco.....	53
2.2.1 Decreto nº 10.046/2019	54
2.2.2 Decreto nº 10.209/2020	58
2.2.3 Portaria RFB nº 34/2021.....	60
2.2.4 Portaria RFB nº 81/2021.....	63
2.2.5 Portaria RFB nº 167/2022.....	64
2.2.6 Convênio ICMS nº 134/2016.....	66
2.3 Mecanismos de proteção de dados	69
2.4 Aplicabilidade das normas de proteção de dados pessoais às trocas de informações tributárias.....	75

CAPÍTULO III

OS STANDARDS PARA A ATUAÇÃO DO FISCO BRASILEIRO NA TRIBUTAÇÃO

MOVIDA A DADOS	82
3.1 Considerações preliminares.....	82
3.2 Coleta de dados.....	85
3.2.1 Juízo de adequação e necessidade: julgamento da ADI nº 6.387	86
3.3 Transferência de dados.....	88
3.3.1 Parâmetros fixados na ADI nº 6.649 e na ADPF nº 695	89
3.3.2 Balizas para o compartilhamento de procedimentos fiscalizatórios com os órgãos de persecução penal.....	95
3.4 Penalidades aplicáveis aos agentes públicos	100
3.5 Diretrizes internacionais e a experiência comparada.....	103
3.5.1 As alterações no Código Tributário alemão.....	107
3.5.2 A interpretação do BVerfG quanto à limitação do sigilo fiscal.....	113
3.5.3 As ponderações acerca da publicização de dados de contribuintes húngaros.....	114
3.5.4 O caso americano <i>Harper v. Rettig</i>	120
3.6 Breves reflexões sobre a Reforma do Sistema Tributário brasileiro	122
CONSIDERAÇÕES FINAIS	124
REFERÊNCIAS	139

INTRODUÇÃO

“Algumas declarações de direitos, ecoando o Artigo 3 da Declaração Universal dos Direitos Humanos, consagram o direito à vida, à liberdade e à segurança na Internet. A dignidade humana não é colocada em risco apenas quando se enfrenta uma ameaça física. Os danos on-line podem ser imateriais, mas não necessariamente menos tangíveis do que os que ocorrem no mundo real.”

(Edoardo Celeste, tradução nossa)¹

Recentemente, parlamentares americanos, sob a liderança da Senadora Elizabeth Warren, endereçaram uma carta ao Procurador-Geral dos Estados Unidos, Merrick Garland, à Presidente da Comissão Federal de Comércio, Lina Khan, ao Comissário da Receita Federal americana, Daniel Werfel, e ao Inspetor-Geral do Tesouro para Administração Tributária, J. Russell George, requerendo a investigação das empresas *H&R Block*, *TaxAct* e *TaxSlayer*, grandes companhias de contabilidade e consultoria tributária, em razão de uma possível prática de transmissão secreta de informações sensíveis de contribuintes à *Meta* e ao *Google*.

Conforme amplamente noticiado², suspeita-se que esses escritórios compartilharam, por anos, dados fiscais de milhões de contribuintes através de provedores de *softwares* de obrigações tributárias, a fim de municiar essas duas

¹ No original: “some declarations of rights, echoing Article 3 of the Universal Declaration of Human Rights, enshrine a right to life, liberty, and security on the Internet. Human dignity is not only imperilled when facing a physical threat. Online harms can be immaterial but may not necessarily be less tangible than those occurring in the real world”. CELESTE, Edoardo. **Digital Constitutionalism: the role of internet bill of rights**. Nova Iorque: Routledge, 2023. p. 176-177.

² FEINER, Lauren. Google and Meta got customer data from tax prep firms, and lawmakers want a probe. **CNBC**. 12 jul. 2023. Disponível em: <https://www.cnbc.com/2023/07/12/google-meta-got-data-from-tax-prep-firms-lawmakers-call-for-probe.html>. Acesso em: 23 jul. 2023.

plataformas para suas atividades de direcionamento de anúncios aos usuários. A carta é fruto de um minucioso estudo realizado por vários meses que, segundo seus subscritores, revelou “uma violação chocante da privacidade do contribuinte por empresas de preparação de impostos [*tax prep companies*] e por grandes empresas de tecnologia que parecem violar os direitos dos contribuintes e podem ter violado a lei de privacidade do contribuinte” (tradução nossa)³.

Essa denúncia deflagra um grave episódio de afronta à privacidade dos contribuintes americanos e exemplifica alguns dos reflexos de uma tendência inerente à nova ordem econômica global.

Com o crescimento dos serviços digitais e as inovações no mercado, o fenômeno da exploração de dados, a exemplo do caso acima, ganhou expressiva relevância no mundo todo. O grande volume de informações armazenadas no “*Big Data*” passou a assumir notório protagonismo nas relações econômicas, e o globo viu surgir um “modelo socioeconômico orientado por dados” (tradução nossa)⁴.

Os dados pessoais se tornaram um novo ativo valioso para as empresas da economia digital⁵. Com isso, surgiram novos modelos de negócios, com estruturas multijurisdicionais, que possibilitam a atuação das empresas em vários mercados “sem que, necessariamente, haja uma presença física tributável em cada uma dessas localidades”⁶. Nesse sentido, as informações fornecidas pelos consumidores passaram a operar como importantes insumos para a consecução dessas atividades⁷.

A título de exemplo, mencionem-se as grandes companhias de publicidade,

³ No original: “*the findings of this report reveal a shocking breach of taxpayer privacy by tax prep companies and by Big Tech firms that appeared to violate taxpayers’ rights and may have violated taxpayer privacy law*”. Disponível em: <https://www.warren.senate.gov/imo/media/doc/2023.07.11%20Letter%20to%20IRS,%20TIGTA,%20FTC,%20DOJ%20on%20tax%20prep%20pixel%20data%20sharing.pdf>. Acesso em: 23 fev. 2023.

⁴ No original: “*as the volume and frequency of collection, use, and storage of personal data intensifies, giving rise to what is commonly referred to as ‘big data’, social and economic relations shift towards a ‘data-driven socioeconomic model’*”. LIOTTI, Belisa Ferreira. Taxpayers’ data protection: do international, regional, and domestic instruments guarantee adequate rights in tax (A)EoI? *Intertax*, v. 50, n. 2, p. 138-158, 2022. p. 138. Disponível em: <https://kluwerlawonline.com/journalarticle/Intertax/50.2/TAXI2022014>. Acesso em: 24 fev. 2023.

⁵ Cf. THIMMESCH, Adam B. Transacting in data: tax, privacy, and the new economy. *Denver Law Review*, v. 94, n. 1, p. 145-194, 2016.

⁶ SILVA, Priscila Stela Mariano da; BOMFIM, Tatiana. Publicidade on-line sob a perspectiva internacional: uma análise dos casos Google no mundo. *In: PISCITELLI, Tathiane (Org.). Tributação da Economia Digital*. São Paulo: Thomson Reuters Brasil, 2018. p. 127-143. p. 127.

⁷ Cf. RAYPORT, Jeffrey F.; SVIOKLA, John J. Exploiting the Virtual Value Chain. *Harvard Business Review*, nov./dez. 1995. Disponível em: <https://hbr.org/1995/11/exploiting-the-virtual-value-chain>. Acesso em: 24 fev. 2023.

que adotam um modelo operacional voltado para a prestação de serviços *on-line*, de forma gratuita, para clientes em todo o mundo (v.g., motores de busca).

Essas operações fornecem à empresa prestadora uma quantidade substancial de dados, incluindo a geolocalização, o histórico de atividades e as informações cadastrais dos usuários. Após os processos de coleta, refinamento, processamento e análise dos dados, torna-se possível o desenvolvimento de um algoritmo que direciona anúncios aos usuários com maior probabilidade de que se desperte o interesse pelos produtos oferecidos. A receita da venda de publicidade, geralmente, é calculada com base no número de usuários que acessam cada anúncio⁸.

Além dessa viabilidade econômica da exploração de informações para o ramo privado, tem-se visto que o próprio Estado é também um relevante usuário de dados. Como ensina Miriam Wimmer, o tratamento de dados pessoais pelo Estado está na “essência das atividades do Poder Público e constitui condição indispensável para o cumprimento de suas missões”⁹.

É o que se verifica a partir da intensificação e da complexificação das operações transnacionais, quando diversas medidas focadas no combate às práticas anticoncorrenciais e/ou ilícitas – tais como evasão fiscal e lavagem de dinheiro – têm sido adotadas para fortalecer a cooperação fiscal e aprimorar a troca de informação (*Exchange of Information – Eol*) entre diferentes jurisdições¹⁰.

Nessa perspectiva, seguindo os avanços tecnológicos, governos e

⁸ Um exemplo desse modelo de negócio é o *Google AdWords*, serviço voltado para a exibição de anúncios dentro das pesquisas realizadas pelo motor de busca da *Google*. O contrato de prestação de serviço prevê, expressamente, que o pagamento é realizado pelo contratante “depois que os seus anúncios receberem os cliques”, que são calculados pelo critério de Custo Por Clique (CPC). Disponível em: <https://support.google.com/google-ads/answer/14074?hl=pt-BR>. Acesso em: 24 fev. 2023. Os anúncios surgem para os usuários da plataforma a partir da busca por palavras-chave previamente selecionadas pelas empresas contratantes. Com essas ferramentas, a publicidade *on-line* atingiu quase que uma onipresença no meio virtual. Cf. Termos do Programa de Publicidade da *Google*. Disponível em: <https://support.google.com/google-ads/answer/14074?hl=pt-BRhttps://www.google.com/intl/pt-BR/adwords/select/TCBrazilForGoogleBrazil1108.html>. Acesso em: 24 fev. 2023. AGUIAR, Luciana Ibiapina Lira. Tributação de marketing digital por meio de *websites*: Caso *Google AdWords* e o contraponto entre as perspectivas brasileira e internacional. In: FARIA, Renato Vilela; SILVEIRA, Ricardo Maitto da; MONTEIRO, Alexandre Luiz Moraes do Rêgo (Orgs.). **Tributação da Economia Digital**: Desafios no Brasil, experiência internacional e novas perspectivas. São Paulo: Saraiva Educação, 2018. p. 570-587. p. 575.

⁹ WIMMER, Miriam. O regime jurídico do tratamento de dados pessoais pelo Poder Público. In: DONEDA, Danilo; SARLET, Ingo Wolfgang; MENDES, Laura Schertel; RODRIGUES JUNIOR, Otavio Luiz (Orgs.). **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021. p. 271-288. p. 271.

¹⁰ A OCDE possui trabalho relevante na construção de políticas globais sobre o assunto, com o seu *Global Forum on Transparency and Exchange of Information for Tax Purposes*. Disponível em: <https://www.oecd.org/tax/transparency/>. Acesso em: 24 fev. 2023.

organizações internacionais têm aperfeiçoado seus procedimentos fiscais, na linha de um processo de automatização de armazenamento e de transmissão periódica de dados pessoais em suas bases. O recente estabelecimento do modelo de troca automática de informação (*Automatic Exchange of Information – AEOI*)¹¹ demonstra essa preocupação.

A partir desses argumentos, é possível notar que a troca de informações tributárias passou a possuir grande relevância nos últimos anos. Concomitantemente, a pressão pela automação desse processo aumentou no cenário internacional, especialmente porque isso passou a ser visto como uma ferramenta necessária à tributação justa e correta¹².

Contudo, como consequência dessa nova abordagem, uma significativa quantidade de dados vem sendo explorada de maneira que não era antes pensada em decorrência dessas inovações. Por conseguinte, há o risco de as regras atuais se tornarem obsoletas e, em certa medida, falharem na busca por uma proteção suficiente¹³.

Com o aumento exponencial do volume de dados tratados, uma das maiores preocupações, no tocante à transferência e à disponibilização de informações fiscais aos grandes *players* da tributação internacional, diz respeito à possibilidade de violação de direitos dos contribuintes, a exemplo dos direitos à privacidade e ao sigilo de dados¹⁴.

Isso porque os modelos atuais de troca de informações – como a história

¹¹ Cf. OCDE. **Automatic Exchange of Information: what it is, how it works, benefits, what remains to be done**. Paris: OECD Publishing, 2012. Disponível em: <https://www.oecd.org/ctp/exchange-of-tax-information/automatic-exchange-of-information-report.pdf> . Acesso em: 24 fev. 2023; RONCO, Stefano Maria. Data Protection in Direct Tax Matters and Developments from the EU Standpoint: The Case of Automatic Exchange of Information. **International Tax Studies (ITAXS)**, v. 3, n. 4, 2020.

¹² OCDE, 2012, p. 19.

¹³ LIOTTI, 2022, p. 139.

¹⁴ Nesse sentido: “[...] a atenção aos direitos do contribuinte é mais necessária agora devido à adoção do novo padrão global de troca automática de informações. Houve uma mudança da troca mediante solicitação para a troca automática de informações (‘AEOI’). Na AEOI, não serão trocadas apenas informações sobre itens específicos de um único contribuinte (ou de um grupo específico de contribuintes), mas também informações em massa. Portanto, os países devem levar em conta que, devido ao ritmo acelerado em que a AEOI ocorrerá, o resultado poderá ser um menor controle sobre a precisão e o uso das informações pelas autoridades receptoras e fornecedoras” (tradução nossa). DEBELVA, Filip.; MOSQUERA VALDERRAMA, Irma Johanna. Privacy and confidentiality in exchange of information procedures: some uncertainties, many issues, but few solutions. **Intertax**, v. 45, n. 5, p. 362-381, 2017. p. 366. Cf., ainda, SCHAPER, Marcel. Data Protection Rights and Tax Information Exchange in the European Union: An Uneasy Combination. **Maastricht Journal of European and Comparative Law**, v. 23, n. 3, p. 514-530, 2016. Disponível em: <https://cris.maastrichtuniversity.nl/en/publications/data-protection-rights-and-tax-information-exchange-in-the-europe>. Acesso em: 24 fev. 2023.

recente evidencia – são propensos a falhas operacionais. A título de exemplo, em 2019, o sistema da *National Revenue Agency* (NRA), da Bulgária, foi hackeado e muitos dos dados armazenados pelo órgão foram vazados. Segundo a nota lançada pela Organização para Cooperação e Desenvolvimento Econômico (OCDE), o governo búlgaro posteriormente confirmou que os dados seriam, de fato, dos sistemas da NRA e que neles havia informações trocadas automaticamente com países parceiros de tratados internacionais¹⁵.

Nessa perspectiva, argumenta-se acerca da necessidade de um instrumento vinculante para todas as jurisdições, que lide especificamente com a salvaguarda dos contribuintes no âmbito da troca automática de informações¹⁶.

Em 2003, o Centro de Política e Administração Fiscais da OCDE publicou a Nota Prática “*Taxpayers’ Rights and Obligations*”, que elencava alguns dos direitos relacionados à proteção dos contribuintes. Dentre eles, foram mencionados: (i) o direito de ser informado, assistido e ouvido; (ii) o direito à certeza; (iii) o direito à privacidade; e (iv) o direito à confidencialidade e ao sigilo¹⁷. Trata-se de relevante iniciativa da organização, que, a despeito da ampla variedade de realidades entre os diferentes países do mundo, visava implementar diretrizes sobre obrigações e direitos básicos, que deveriam ser observadas por toda e qualquer autoridade fiscal.

No que tange à salvaguarda do direito à confidencialidade, a OCDE lançou, em 2012, um guia para essa finalidade no âmbito da troca de informações para fins fiscais. Intitulado de “*Keeping It Safe*”, o relatório fornece orientações gerais sobre como as administrações tributárias deveriam proteger o sigilo das informações dos contribuintes, tanto internamente quanto externamente, com os instrumentos de troca de informações¹⁸.

Embora a OCDE tenha demonstrado sua preocupação com a necessidade de se buscar equilibrar os interesses entre as partes envolvidas, os trabalhos desenvolvidos pela organização, por serem apenas diretrizes, não trazem o *enforcement* que o tema demanda¹⁹.

Isso evidencia que os instrumentos desenhados como novas alternativas à

¹⁵ Disponível em: <https://www.oecd.org/tax/transparency/documents/statement-on-the-data-breach-in-the-national-revenue-agency-of-bulgaria.htm>. Acesso em: 13 mar. 2023.

¹⁶ LIOTTI, 2022, p. 143.

¹⁷ Disponível em: [https://www.oecd.org/tax/administration/Taxpayers' Rights and Obligations-Practice_Note.pdf](https://www.oecd.org/tax/administration/Taxpayers%27_Rights_and_Obligations-Practice_Note.pdf). Acesso em: 13 mar. 2023.

¹⁸ Disponível em: <https://www.oecd.org/ctp/exchange-of-tax-information/keeping-it-safe-report.pdf>. Acesso em: 13 mar. 2023.

¹⁹ LIOTTI, *op. cit.*, p. 143.

AEoI não asseguram uma efetiva expectativa de proteção de dados dos contribuintes. Hoje, muitos dos mecanismos reservam a adequação dessa salvaguarda apenas aos parâmetros fixados pelas leis de cada país, o que não solucionaria o problema no âmbito global, haja vista que essas normas internas não são vinculantes para os outros Estados.

Dessa maneira, ainda é nebuloso o cenário em relação à garantia de direitos dos contribuintes nessas operações. O enfrentamento desse desafio é urgente, eis que o incremento na transmissão de informações intensifica os riscos para os dados pessoais, haja vista que, quanto mais informação é trocada, maior a possibilidade de quebras de privacidade e de confidencialidade.

Outrossim, o debate se mostra premente neste momento em que medidas relevantes têm sido adotadas para fortalecer a proteção dos usuários no ciberespaço. Essas providências, invariavelmente, devem ser ponderadas em conjunto com as medidas impostas no âmbito tributário.

Na União Europeia (UE), a proteção de dados foi reconhecida como um direito fundamental em suas primeiras leis. Adicionalmente, a UE também implementou a Diretiva da Proteção de Dados, em 1995, que veio a ser posteriormente substituída pelo Regulamento Geral sobre a Proteção de Dados (RGPD) (*General Data Protection Regulation – GDPR*), em 2016²⁰.

Por sua vez, no Brasil, com a Proposta de Emenda à Constituição (PEC) nº 17/2019, o poder constituinte derivado incluiu a proteção de dados pessoais no rol dos direitos fundamentais, ratificando, assim, o *status* constitucional dessa garantia²¹. Ademais, inspirado no RGPD, o país aprovou a sua Lei Geral de Proteção de Dados Pessoais (LGPD)²², que elenca regras gerais para o tratamento de dados pessoais voltadas para a proteção dos direitos fundamentais de liberdade

²⁰ UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). **Jornal Oficial da União Europeia**, L 119, p. 1-88, 4 maio 2016. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679>. Acesso em: 20 maio 2023.

²¹ “Art. 5º [...] LXXIX - é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais (Incluído pela Emenda Constitucional nº 115, de 2022).” BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988**. Brasília: Presidência da República, [2022]. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm. Acesso em: 24 fev. 2023.

²² BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília: Presidência da República, [2018]. Disponível em: https://www.planalto.gov.br/ccivil_03/ato2015-2018/2018/lei/113709.htm. Acesso em: 24 fev. 2023.

e de privacidade e do livre desenvolvimento da personalidade da pessoa natural (art. 1º).

Por outro lado, como membro do *Global Forum on Transparency and Exchange of Information for Tax Purposes Peer Review*²³ desde 2009, o Brasil precisa estar empenhado em implementar o modelo internacional de transparência e troca de dados para fins fiscais. Nesse particular, a Secretaria Especial da Receita Federal do Brasil (RFB) e as Fazendas Públicas estaduais e municipais dispõem de recursos e amplos poderes para a obtenção e a transmissão de informações tributárias.

Aliás, o art. 199, *caput*, do Código Tributário Nacional (CTN) prevê que as Fazendas Públicas dos Entes Federativos deverão prestar assistência mútua para a fiscalização dos tributos respectivos, com a expressa previsão sobre a troca de informações na forma estipulada em leis ou convênios. Da mesma forma, o parágrafo único desse dispositivo versa sobre a permissão de permuta de informações entre a União e os Estados estrangeiros, observando-se os tratados, acordos e convênios e visando o interesse de arrecadação e fiscalização de tributos²⁴.

Além disso, o Brasil possui, hoje, mais de trinta acordos contra a bitributação²⁵, que estipulam cláusulas de Eol. Contudo, nem todos observam integralmente o padrão previsto pelo art. 26 do Modelo de Convenção Fiscal (*Model Tax Convention*) da OCDE, que trata especificamente da troca de informações entre

²³ Trata-se de projeto da OCDE voltado para monitorar e revisar a implementação do padrão internacional de requisição de troca de informações (EolR) e de troca automática de informações (AEol) no mundo. O fórum utiliza um sistema de revisão por pares (*peer review*) para examinar as estruturas legais e regulatórias de cada um de seus 168 membros (informação de agosto de 2023). Entre 2010 e 2016, foi realizada a sua primeira rodada, com enfoque na revisão das estruturas legais e regulatórias de cada jurisdição. Em 2016, a organização iniciou a segunda rodada, direcionada para a revisão dos sistemas internos de cada país, a fim de se garantir a conformidade contínua no estabelecimento desse modelo. Disponível em: https://www.oecd-ilibrary.org/taxation/global-forum-on-transparency-and-exchange-of-information-for-tax-purposes-peer-reviews_2219469x?page=1. Acesso em: 2 ago. 2023.

²⁴ “Art. 199. A Fazenda Pública da União e as 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.” BRASIL. **Lei nº 5.172, de 25 de outubro de 1966**. Dispõe sobre o Sistema Tributário Nacional e institui normas gerais de direito tributário aplicáveis à União, Estados e Municípios. Brasília: Presidência da República, [1966]. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l5172.htm. Acesso em: 24 fev. 2023.

²⁵ Disponível em: <https://www.gov.br/receitafederal/pt-br/aceso-a-informacao/legislacao/acordos-internacionais/acordos-para-evitar-a-dupla-tributacao/acordos-para-evitar-a-dupla-tributacao>. Acesso em: 24 fev. 2023.

os países signatários^{26 27}.

Nessa linha, o Estado brasileiro também ratificou o novo texto da *Convenção sobre Assistência Mútua Administrativa em Matéria Tributária*, por meio do Decreto nº 8.842, de 29 de agosto de 2016²⁸. O ato foi emendado pelo Protocolo de 1º de junho de 2010 e assinado pelo então Ministro da Fazenda, Guido Mantega, em 3 de novembro de 2011, no âmbito da Cúpula de Cannes do G20. Segundo a mensagem do titular da pasta, submetida à apreciação do Congresso Nacional, o texto visa “promover a cooperação em matéria fiscal no âmbito multilateral, equilibrando o intercâmbio de informações entre as autoridades tributárias signatárias com rigoroso respeito aos direitos fundamentais do contribuinte”²⁹.

Todavia, embora se tenha visto importantes avanços em relação à cooperação e à fiscalização tributária, ainda se discute se esses mecanismos estariam em harmonia com as mencionadas regras de proteção de dados pessoais dos cidadãos brasileiros.

Ao passo que não há como transladar o regime jurídico da proteção de dados das relações privadas para o contexto da troca de informações entre o contribuinte e o Estado, ante as diferentes complexidades do tratamento interno pela Administração Pública, verifica-se a ausência de parâmetros bem definidos para atuação da autoridade tributária no ambiente digital, haja vista a carência de normas e instruções que busquem suficientemente estabelecer um diálogo entre a proteção de dados e o poder-dever fiscalizatório estatal.

É nesse contexto que o tema desta pesquisa se insere: neste trabalho, é feito um exame do estado da arte dos *standards* para o tratamento de dados de contribuintes. A partir disso, o *objetivo geral* da dissertação é justamente o de propor mecanismos, políticas e parâmetros tributários para o problema, por meio da conjugação do estudo das operações de dados com a investigação das diferentes

²⁶ Disponível em: <https://www.oecd.org/ctp/treaties/articles-model-tax-convention-2017.pdf>. Acesso em: 24 fev. 2023.

²⁷ LIOTTI, 2022, p. 141.

²⁸ BRASIL. **Decreto nº 8.842, de 29 de agosto de 2016**. Promulga o texto da Convenção sobre Assistência Mútua Administrativa em Matéria Tributária emendada pelo Protocolo de 1º de junho de 2010, firmada pela República Federativa do Brasil em Cannes, em 3 de novembro de 2011. Brasília: Presidência da República, [2016]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/D8842.htm. Acesso em: 24 fev. 2023.

²⁹ Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1278463&filename=MSC%20270/2014. Acesso em: 24 fev. 2023.

perspectivas relativas à atuação do Fisco nas plataformas digitais, à luz dos critérios de proteção de dados definidos no ordenamento brasileiro e nas diretrizes internacionais.

A abordagem é relevante, considerando (i) a incipiência do debate na academia jurídica brasileira, que ainda carece de estudos voltados para a tributação na economia digital e (ii) a necessidade de que se tenha balizas bem definidas sobre o tema, haja vista que a digitalização dos modelos de negócios é um fenômeno intrínseco à Era da Informação e, dessa forma, é essencial que sejam fixadas regras acerca da relação entre tributação e proteção de dados, a fim de se resguardar a segurança jurídica dos contribuintes no que tange à salvaguarda da privacidade.

Em linhas gerais, este trabalho é dividido em duas partes: uma *teórica*, voltada para o estudo dos principais conceitos que circundam a temática em exame, notadamente as garantias individuais dos contribuintes e as regras vigentes sobre o uso de informações fiscais; e outra *propositiva*, endereçando as práticas nacionais e internacionais acerca dos critérios para a atuação da Administração Tributária no bojo das operações de coleta e de compartilhamento de dados.

No *primeiro capítulo*, de cunho predominantemente descritivo, são definidos os direitos à privacidade e ao sigilo fiscal. Os tópicos partem do exame dos julgamentos e estudos mais relevantes, que buscaram conceitualizar esses institutos. Após perpassar por esses *leading cases* e pelas compreensões doutrinárias, é feita uma investigação teórica sobre a ressignificação dessas garantias no âmbito das operações com dados pessoais. Nesse sentido, investiga-se, a partir das transformações decorrentes das inovações tecnológicas, a nova noção de privacidade, a qual é orientada pela ideia de autodeterminação informativa. Ademais, também são tecidas considerações sobre a sua aplicabilidade na seara tributária.

Posteriormente, no *segundo capítulo*, é examinado o arcabouço normativo brasileiro sobre proteção de dados dos contribuintes. Nesse particular, aborda-se o processo de coleta de informações pelo Fisco à luz das normas vigentes. Após, são descritas as diretrizes da LGPD para, assim, definir seu alcance no campo das trocas de informações tributárias.

O *terceiro capítulo*, por sua vez, visa analisar e propor os *standards* para a atuação da Administração Tributária brasileira na economia movida a dados. Com isso, essa seção subdivide-se em cinco subcapítulos. No *primeiro*, são discutidos os

parâmetros para a atuação da Fazenda Pública no âmbito da coleta de dados. Em seguida, no *segundo* tópico, discorre-se sobre as balizas para as operações de transmissão de informações a outros pelo órgão fazendário. Já no *terceiro* subcapítulo, apresentam-se as penalidades aplicáveis aos agentes públicos no âmbito dessas operações com dados intermediadas pelo Fisco. O *quarto* ponto versa sobre exemplos advindos da experiência comparada e algumas das normas internacionais do assunto. Na *quinta* parte, são tecidas, por oportuno, breves considerações acerca da necessidade de o debate acompanhar os assuntos abordados na vindoura Reforma Tributária.

Por fim, a título de *conclusão*, pondera-se que o argumento da mera preservação do sigilo fiscal é insuficiente para legitimar, *per se*, o uso ilimitado de dados pessoais pela Administração Tributária. Partindo-se de uma análise da proteção de dados como uma garantia dinâmica e permanente não só da confidencialidade, mas também da privacidade em sua concepção mais atual – a qual se projeta como um poder decisório do indivíduo em relação às suas informações pessoais –, conclui-se que o dever fiscalizatório estatal e as finalidades a ele inerentes não podem operar como permissões imoderadas para os “superprocessamentos” de informações fiscais. Assim, a atividade tributária encontrará seus limites nas garantias individuais dos contribuintes.

CAPÍTULO I

AS GARANTIAS CONSTITUCIONAIS DOS CONTRIBUINTES

“Adotar uma interpretação comunitária do valor da privacidade significa que a defesa da privacidade e a proteção dos dados pessoais são vistas como sendo de interesse público por direito próprio, ou seja, que há um valor público no respeito aos dados pessoais per se.”

(Gillian Black e Leslie Stevens, tradução nossa)³⁰

1.1 Considerações preliminares

Com as recentes crises financeiras globais e os novos modelos de negócios da economia movida a dados, os países do globo enfrentaram grandes desafios no combate à perda de receita. À vista disso, os Estados têm se empenhado, principalmente, em fomentar o *compliance* de dados fiscais e em combater os planejamentos tributários arrojados, que exploram as diferenças existentes entre as leis tributárias de cada país, com a finalidade de redução da carga tributária³¹.

Consciente do fenômeno da erosão da base tributária ocasionado pelas novas relações de comércio, a OCDE publicou, em 2013, um relatório intitulado de “*Base Erosion and Profit Shifting*” (BEPS)³². O BEPS foi endereçado aos líderes do G20 e aborda as principais problemáticas decorrentes dessa nova realidade,

³⁰ No original: “*Adopting a communitarian interpretation of the value of privacy means that upholding privacy and protecting personal data is seen as being in the public interest in its own right, ie that there is a public value in respecting personal data per se*”. BLACK, Gillian; STEVENS, Leslie. Enhancing data protection and data processing in the public sector: the critical role of proportionality and the public interest. **SCRIPTed**, v. 10, n. 1, p. 93-122, 2013. p. 117.

³¹ COCKFIELD, Arthur J. International Tax Transparency. **Perspectives on Tax Law and Policy**, v. 1, n. 4, p. 1-17, dez. 2020. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3753715. Acesso em: 20 maio 2023.

³² OCDE. **Combate à Erosão da Base Tributária e à Transferência de Lucros**. Paris: OECD Publishing, 2013. Disponível em: https://read.oecd-ilibrary.org/taxation/combate-a-erosao-da-base-tributaria-e-a-transferencia-de-lucros-portuguese-version_9789264201248-pt#page1. Acesso em: 24 fev. 2023.

buscando propor políticas fiscais de cooperação internacional para o combate aos arranjos tributários abusivos.

Com o BEPS, foi idealizado um sistema de relatórios, “país por país” (*Country-by-Country Reporting – CbC*), que impôs às grandes empresas multinacionais a divulgação dos pagamentos de suas obrigações tributárias em todos os locais que operam. Um outro evento catalisador foi a série de episódios envolvendo “megavazamentos” de dados em paraísos fiscais. Essas quebras de sigilo ligaram o alerta global em relação ao elevado grau de perda de receita decorrente das evasões fiscais: viu-se que as grandes companhias estariam enviando seus recursos a esses países com regras tributárias mais flexíveis³³.

Por conta disso, foram formuladas políticas internacionais voltadas à troca de informações fiscais; seja ela automática, mediante solicitação ou espontânea. Contudo, em contrapartida, os sonegadores “tomaram os passos necessários para combater essas medidas; eles começaram a usar paraísos fiscais que não tinham acordos de troca de informações com outros países”³⁴.

Diante desses desafios, para que se possa alcançar os objetivos perquiridos pelos Estados, tendo em vista as dificuldades acima narradas, verifica-se a importância de se buscar equilibrar os direitos individuais dos contribuintes com os deveres estatais de arrecadação e de combate à sonegação. Com isso, é imprescindível que, em um primeiro momento, sejam bem estabelecidos os limites e os conceitos dos dados a serem transmitidos no bojo das obrigações tributárias.

Nesse contexto, faz-se necessário examinar a abrangência da privacidade e do sigilo fiscal.

Muito por conta das construções históricas e dos receios em relação à atividade fiscalizadora das autoridades, que era muito ligada a um poder impositivo de confisco para o pagamento de tributos, as informações do contribuinte, ao lado dos dados financeiros, têm sido tradicionalmente consideradas uma das facetas mais sensíveis da privacidade.

As informações fiscais podem abarcar dados pessoais detalhados sobre a identidade e o comportamento de um indivíduo. A título de exemplo, “as informações sobre a declaração de imposto de renda podem incluir informações sobre, entre outras coisas, a renda de um indivíduo, seus dependentes, sua condição de saúde e

³³ COCKFIELD, 2020, p. 1-2.

³⁴ *Ibid.*, p. 1-2.

deficiência e doações políticas” (tradução nossa)³⁵.

Nessa mesma perspectiva, o sigilo fiscal opera como garantia essencial ao direito à privacidade no âmbito do direito tributário. Conforme será abordado neste capítulo, é necessário fixar regras sobre o assunto, de modo a garantir o correto funcionamento do Estado no campo da tributação.

1.2 Direito à privacidade

A privacidade é um “conceito em desordem”, pois, por ser abstrata e subjetiva, comporta diferentes significados, a depender da situação. Atualmente, o instituto traz consigo uma compreensão abrangente, “que engloba (entre outras coisas) liberdade de pensamento, controle sobre o corpo, solidão em casa, controle sobre informações pessoais, liberdade de vigilância, proteção da reputação e proteção contra buscas e interrogatórios”³⁶.

No que tange às relações com a Administração Pública, que envolvem o tratamento de dados dos cidadãos, a privacidade passou a guardar correlação com a noção de autodeterminação informativa. Sob esse aspecto, essa garantia decorre de um direito geral de personalidade³⁷. Seu âmbito de proteção abarca não apenas os dados referentes ao núcleo dos direitos de personalidade, mas também os “dados que, por sua natureza, são extremamente sensíveis e, portanto, devem ser protegidos”³⁸.

No entanto, essa concepção já ganhou diferentes interpretações no passado e evoluiu com o tempo. Sua compreensão histórica costuma ser ligada à publicação do artigo “*The Right to Privacy*”, de autoria dos juristas Samuel Warren e Louis

³⁵ COCKFIELD, Arthur J. Sharing Tax Information in the 21st Century: Big Data Flows and Taxpayers as Data Subjects. **Canadian Tax Journal**, v. 67, n. 4, p. 1179-1199, 2019. p. 1189.

³⁶ No original: “*Privacy, however, is a concept in disarray. Nobody can articulate what it means. Currently, privacy is a sweeping concept, encompassing (among other things) freedom of thought, control over one’s body, solitude in one’s home, control over personal information, freedom from surveillance, protection of one’s reputation, and protection from searches and interrogations*”. SOLOVE, Daniel J. **Understanding Privacy**. Cambridge: Harvard University Press, 2008. p. 1.

³⁷ ALEMANHA. **Lei Fundamental da República Federal da Alemanha, de 23 de maio de 1949**. Berlim: Parlamento Federal Alemão, [2019]. Disponível em: <https://www.bundestag.de/pt>. Acesso em: 5 out. 2023. (Grundgesetz, art. 2, par. 1, p. 16).

³⁸ SEER, Roman. Proteção de dados e tributação na Alemanha: repercussões do Regulamento Geral sobre Proteção de Dados. Tradução de Diogo Brandau Signoretti. **Revista Jurídica da Presidência**, Brasília, v. 22, n. 126, p. 20-47, fev./maio 2020. p. 23. Disponível em: <https://revistajuridica.presidencia.gov.br/index.php/saj/article/view/2128/1331>. Acesso em: 20 maio 2023.

Brandeis, no final do século XIX. Segundo os autores³⁹:

Esse direito é totalmente independente do material no qual, ou dos meios pelos quais, o pensamento, sentimento ou emoção é expresso. Ele pode existir independentemente de qualquer ser corpóreo, como em palavras faladas, uma canção cantada, um drama representado. Ou, se expresso em qualquer material, como em um poema escrito, o autor pode ter se separado do papel, sem perder qualquer direito de propriedade sobre a composição em si (tradução nossa).

Tal definição possibilitou, a partir de uma leitura dos precedentes do *common law*, que se formasse a visão de um direito imaterial, desvinculado da clássica ideia de proteção da propriedade.

Na doutrina brasileira, os estudos acerca da identificação do direito à privacidade apontaram, inicialmente, para a abordagem do professor Tércio Sampaio Ferraz Júnior, em seu clássico trabalho “Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado”, publicado em 1993. Naquele artigo, o professor Tércio pontuava que a privacidade guardaria correlação com uma interpretação da inviolabilidade do sigilo sob o prisma da comunicação de dados. Assim, nessa concepção, o âmbito de proteção dessa inviolabilidade impediria “o acesso à própria ação comunicativa, mas não aos dados comunicados”⁴⁰.

Trata-se, então, de uma perspectiva voltada para a conceituação da privacidade como um direito negativo de não intervenção nas situações de trânsito de dados. Essa ideia encetou, inclusive, o primeiro entendimento jurisprudencial do STF sobre o tema.

1.2.1 Evolução jurisprudencial do STF acerca da correlação da privacidade com a inviolabilidade do sigilo

³⁹ No original: “*This right is wholly independent of the material on which, or the means by which, the thought, sentiment, or emotion is expressed. It may exist independently of any corporeal being, as in words spoken, a song sung-, a drama acted. Or if expressed on any material, as a poem in writing, the author may have parted with the paper, without forfeiting any proprietary right in the composition itself*”. WARREN, Samuel D.; BRANDEIS, Louis D. *The Right to Privacy*. **Harvard Law Review**, v. 4, n. 5, p. 193-220, 1890. p. 199. Disponível em: <https://www.jstor.org/stable/1321160>. Acesso em: 20 maio 2023.

⁴⁰ FERRAZ JÚNIOR, Tércio. Sigilo de dados: o direito à privacidade e os limites da função fiscalizadora do Estado. **Revista da Faculdade de Direito da Universidade de São Paulo**, v. 88, p. 439-459, 1993. p. 452. Disponível em: <https://www.revistas.usp.br/rfdusp/article/view/67231>. Acesso em: 20 maio 2023.

Foi com base nessa ideia de não interferência que o Ministro Sepúlveda Pertence proferiu seu voto no Mandado de Segurança (MS) nº 21.729/DF⁴¹ e no Recurso Extraordinário (RE) nº 418.416/SC⁴², este de sua relatoria.

O MS nº 21.729/DF foi impetrado pelo Banco do Brasil S/A contra ofício do então Procurador-Geral da República, que requeria o fornecimento de lista de nomes dos beneficiários de liberação de recursos, em caráter emergencial, ao setor sucroalcooleiro, além de dados sobre “os favorecidos com os créditos em débito para com o Banco, pedindo-se deste, ainda, esclarecimentos sobre a natureza das operações e as respectivas situações”⁴³.

Naquele julgamento, os Ministros Francisco Rezek e Sepúlveda Pertence firmaram entendimento – com base na doutrina de Tércio Sampaio Ferraz Júnior – de que as operações bancárias não restariam abarcadas pelo sigilo de dados. Nessa senda, não haveria quebra de sigilo, “mas a revelação de algo que não só não estava sujeita ao sigilo, como para o qual se recomendava a publicidade”⁴⁴. Assim, a salvaguarda do sigilo de dados alcançaria apenas as comunicações, e não os dados armazenados em dispositivo.

Já no RE nº 418.416/SC, interposto pelo empresário Luciano Hang, buscava-se a cassação da condenação do recorrente por crimes tributários, “dado que fundada em prova obtida por meio ilícito, consubstanciada na decisão que autorizou a busca e apreensão, de cuja execução também teria resultado violação à proteção constitucional ao sigilo das comunicações de dados”⁴⁵.

O tribunal assentou a tese de que a proteção a que se refere o art. 5º, inciso XII, da Constituição Federal seria a da “comunicação ‘de dados’, e não dos ‘dados em si mesmos’, ainda quando armazenados em computador”⁴⁶. Em seu voto, o Ministro Pertence ressaltou que a quebra de sigilo se daria apenas durante a transmissão de informações, isto é, na interceptação das comunicações.

⁴¹ BRASIL. Supremo Tribunal Federal. **MS nº 21.729/DF**. Rel. Min. Marco Aurélio, Redator p/ acórdão Min. Néri da Silveira. Brasília, DF, Plenário, j. 5/10/1995, *DJ* 19/10/2001. Disponível em: <https://jurisprudencia.stf.jus.br/pages/search/sjur101299/false>. Acesso em: 5 out. 2023.

⁴² BRASIL. Supremo Tribunal Federal. **RE nº 418.416/SC**. Rel. Min. Sepúlveda Pertence. Brasília, DF, Plenário, j. 10/5/2006, *DJ* 19/12/2006. Disponível em: <https://jurisprudencia.stf.jus.br/pages/search/sjur92577/false>. Acesso em: 5 out. 2023.

⁴³ BRASIL, ref. 41.

⁴⁴ BRASIL, ref. 41.

⁴⁵ BRASIL, ref. 42.

⁴⁶ BRASIL, ref. 42.

Desse modo, concluiu a Corte que o acesso à base física na qual se encontravam os dados, mediante prévia decisão autorizativa de apreensão, não contrastaria com a ideia da proteção do sigilo de dados, eis que, do contrário, qualquer investigação administrativa seria obstada.

Ainda nessa linha de ideias, a Segunda Turma da Suprema Corte, ao julgar o *Habeas Corpus* (HC) nº 91.867/PA, seguiu o mesmo direcionamento⁴⁷. Os pacientes, denunciados por suposta prática de crime de homicídio qualificado e associação criminosa, pediam o trancamento da ação penal ou, subsidiariamente, o desentranhamento do feito das provas alegadamente produzidas por meios ilícitos.

A Turma ressaltou que a comunicação telefônica não se confundiria com os registros telefônicos, os quais receberiam, inclusive, proteção jurídica distinta. Dessa forma, afastou-se, mais uma vez, a interpretação da cláusula do art. 5º, inciso XII, da Constituição Federal no sentido de proteção aos dados enquanto registro.

Contudo, tal interpretação ganhou novos contornos com os julgados mais recentes dos Tribunais Superiores. Houve, nessa perspectiva, uma possível guinada jurisprudencial em face do atual contexto tecnológico⁴⁸.

Mencione-se, por exemplo, o julgamento do HC nº 168.052/SP⁴⁹, de relatoria do Ministro Gilmar Mendes. Naquele caso, o Ministro Relator ressaltou, expressamente, a superação de seu entendimento anteriormente firmado no HC nº 91.867/PA.

O caso concreto envolvia a obtenção da prova por meio de acesso, sem autorização judicial, a aparelho celular, o que fez com que as autoridades policiais

⁴⁷ BRASIL. Supremo Tribunal Federal. **HC nº 91.867/PA**. Rel. Min. Gilmar Mendes. Brasília, DF, Segunda Turma, j. 24/4/2012, *DJ* 20/9/2012. Disponível em: <https://jurisprudencia.stf.jus.br/pages/search/sjur214794/false>. Acesso em: 5 out. 2023. Nesse mesmo sentido, *cf.*: BRASIL. Supremo Tribunal Federal. **HC nº 124.322 AgR/RS**. Rel. Min. Roberto Barroso. Brasília, DF, Primeira Turma, j. 9/12/2016, *DJ* 19/12/2016. Disponível em: <https://jurisprudencia.stf.jus.br/pages/search/sjur362409/false>. Acesso em: 5 out. 2023; BRASIL. Supremo Tribunal Federal. **RHC nº 132.062/RS**. Rel. Min. Marco Aurélio. Brasília, DF, Primeira Turma, j. 22/11/2016, *DJ* 24/10/2017. Disponível em: <https://jurisprudencia.stf.jus.br/pages/search/sjur375834/false>. Acesso em: 5 out. 2023.

⁴⁸ FONSECA, Reynaldo Soares da; FONSECA, Gabriel Campos Soares da; SANTOS, João Gabriel Costa dos. Jurisdição Constitucional e novas tecnologias: releituras do art. 5º, inciso XII, da Constituição na jurisprudência do Supremo Tribunal Federal. *In*: MENDES, Gilmar Ferreira; PIMENTA DE FREITAS, Matheus (Orgs.). **Constituição, Direito Penal e Novas Tecnologias**. São Paulo: Almedina Brasil, 2023.

⁴⁹ BRASIL. Supremo Tribunal Federal. **HC nº 168.052/SP**. Rel. Min. Gilmar Mendes. Brasília, DF, Segunda Turma, j. 20/10/2020, *DJ* 2/12/2020. Disponível em: <https://jurisprudencia.stf.jus.br/pages/search/sjur437471/false>. Acesso em: 5 out. 2023.

tomassem ciência das conversas havidas no aplicativo *WhatsApp*, cujo teor originou a ação de busca e apreensão na residência do paciente⁵⁰.

Segundo os autos daquele processo, os agentes policiais verificaram, no aplicativo de troca de mensagens, as comunicações que indicavam a traficância, o que os levou a ingressar no domicílio do investigado, local em que drogas e armas foram encontradas. E foi justamente essa sequência de fatos que gerou uma ação penal, com a consequente condenação do paciente. Ocorre que, supostamente, sem o acesso às mensagens de *WhatsApp* dos investigados, os agentes policiais provavelmente não teriam dado início a essa cadeia causal.

O Ministro Gilmar Mendes ressaltou que o caso concreto merecia uma conclusão distinta dos precedentes acima citados por três motivos: (i) as mudanças nas circunstâncias fáticas e jurídicas; (ii) a promulgação de leis posteriores, como a LGPD e o Marco Civil da Internet (Lei nº 12.965/2014); e (iii) “o significativo desenvolvimento das tecnologias da comunicação, do tráfego de dados e dos aparelhos *smartphones*”. Desse modo, esses três fatores sustentariam a ocorrência de uma mutação constitucional⁵¹.

Nessa senda, a proteção da intimidade e da vida privada, contida no art. 5º, inciso X, da Constituição Federal, o princípio da proporcionalidade nas intervenções estatais e o novo contexto tecnológico exigiriam que esse acesso fosse condicionado à prévia decisão judicial, nos termos do art. 5º, inciso XII, da CF. Como bem sintetizam Rafael Mafei e Paula Pedigoni⁵²:

Já não faz sentido distinguir entre dados em trânsito e dados estáticos como critério para maior ou menor proteção à privacidade: o barateamento do armazenamento de dados e a migração das comunicações humanas para serviços providos pela Internet, com opções de armazenamento de segurança em servidores (*backups* na nuvem), torna o conjunto de dados armazenados sobre um indivíduo, por seu considerável volume e abrangência temporal, mais sensível à sua intimidade do que conversas telefônicas interceptadas. [...]

Se não é possível ignorar a distinção entre os incisos X e XII do art. 5º da Constituição, tampouco há razão para impor uma proteção menos efetiva à nossa intimidade apenas porque estejam em dados armazenados, e não em trânsito.

⁵⁰ BRASIL, ref. 49.

⁵¹ BRASIL, ref. 49.

⁵² QUEIROZ, Rafael Mafei Rabelo; PONCE, Paula Pedigoni. Tércio Sampaio Ferraz Júnior e Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado: o que permanece e o que deve ser reconsiderado. **Revista Internet & Sociedade**, São Paulo, v. 1, n. 1, p. 64-90, fev. 2020. p. 80.

Essa inovação jurisprudencial é reflexo das profundas mudanças pelas quais a concepção do direito à privacidade tem passado. O direito que antes era visto como garantia individual de abstenção do Estado na esfera privada (“direito de ser deixado em paz”) foi drasticamente reinventado no novo panorama tecnológico. Passou-se a pensar em um “direito de controle sobre as informações”⁵³, como será abordado a seguir.

1.2.2 Privacidade como autodeterminação informativa

Ligada ao desenvolvimento do conceito de autodeterminação informativa⁵⁴ – mencionado, inicialmente, na paradigmática decisão do *Bundesverfassungsgericht* (BVerfG) sobre a Lei do Censo de 1983⁵⁵ –, a nova conceitualização da privacidade opera “como um contraponto a qualquer contexto concreto de coleta, processamento ou transmissão de dados passível de configurar situação de perigo”⁵⁶.

Desse modo, abandona-se o conteúdo e passa-se a considerar as possibilidades e as finalidades do processamento de dados para a proteção do direito à privacidade. Na atual sociedade em rede⁵⁷, considerando-se a importância dos dados no processamento automatizado de informações de caráter pessoal, observa-se o risco justamente no intuito e nas oportunidades das operações, e não

⁵³ RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008. p. 15-17.

⁵⁴ Cf. MENDES, Laura Schertel Ferreira. Autodeterminação informativa: a história de um conceito. **Revista de Ciências Jurídicas Pensar**, Fortaleza, v. 25, n. 4, p. 1-18, out./dez 2020. Disponível em: <https://ojs.unifor.br/rpen/article/view/10828/pdf>. Acesso em: 20 maio 2023.

⁵⁵ Disponível em: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/1983/12/rs19831215_1_bvr020983en.html;jsessionid=27BB1B55B8E909DFDD46DB2D2AD88A2E.internet012. Acesso em: 25 maio 2023.

⁵⁶ MENDES, Gilmar Ferreira. O direito fundamental à proteção de dados pessoais e a abertura da ordem constitucional à transformação tecnológica: análise do julgamento da ADI 6.387. *In*: ROCHA, Maria Elizabeth Guimarães Teixeira; BASTOS, Ana Carolina Andrada Arrais Caputo; SILVA, Christine Oliveira Peter da; SILVA, Cristina Maria Gama Neves da; D’ALBUQUERQUE, Julia de Baére Cavalcanti; OLIVEIRA, Manuela Simões Falcão Alvim de (Orgs.). **Ela Pedre Vista**: estudos em homenagem à Ministra Rosa Weber. Londrina: Thoth, 2023. p. 329-348. p. 339.

⁵⁷ Segundo Manuel Castells, “[u]ma sociedade em rede é uma sociedade cuja estrutura social é feita de redes alimentadas por tecnologias de informação e comunicação baseadas em microeletrônica”. No original: “A network society is a society whose social structure is made of networks powered by microelectronics-based information and communication technologies”. CASTELLS, Manuel. **The network society**: a cross-cultural perspective. Cheltenham: Edward Elgar Publishing Limited, 2004. p. 3.

no tipo de dado a ser tratado⁵⁸.

Conforme ensina a professora Laura Schertel, com a tecnologia permitindo o armazenamento e processamento eficiente de dados pessoais, “dá-se a associação entre proteção à privacidade e informações pessoais”. Houve, nesse cenário, “uma alteração não apenas do conteúdo do direito à privacidade, mas também do seu léxico, passando a ser denominada privacidade informacional, proteção de dados pessoais autodeterminação informativa, entre outros”⁵⁹.

Com isso, idealizou-se uma garantia que visa tutelar o direito do indivíduo de manter o controle sobre o uso de suas próprias informações. Essa concepção demanda uma releitura do direito à privacidade, tendo por base as transformações digitais e o protagonismo que a informação pessoal em si passou a ter. Como adverte Lawrence Lessig, com a mudança dos paradigmas tecnológicos, as esferas de liberdade precisam ser recriadas para que as garantias constitucionais não sejam esvaziadas⁶⁰.

Tal preocupação não se limita à noção de esfera privada. No âmbito do direito tributário, em que se costuma mitigar a privacidade em prol da eficiência dos serviços públicos de fiscalização e de arrecadação, a Administração encontra contrapesos na nova concepção de intimidade⁶¹.

Roman Seer explica que essa faceta da privacidade também alcança “elementos individualizáveis da tributação, os quais são grandezas econômicas (faturamento, lucro, renda, entre outros) resultantes de ganhos em um mercado aberto”. As informações que devem ser prestadas pelos contribuintes, por proporcionarem “um vasto panorama sobre as relações pessoais, sobre o estilo de vida e sobre as relações profissionais, empresariais e corporativas, além de outras relações econômicas”, também são englobadas nesse âmbito de proteção. Mesmo que os dados apresentem baixo conteúdo informativo, pode haver considerável intervenção na liberdade individual com as técnicas de tratamento e cruzamento de

⁵⁸ MENDES, Laura Schertel Ferreira. Autodeterminação informativa: a história de um conceito. **Revista de Ciências Jurídicas Pensar**, Fortaleza, v. 25, n. 4, p. 1-18, out./dez. 2020. p. 11. Disponível em: <https://ojs.unifor.br/rpen/article/view/10828/pdf>. Acesso em: 20 maio 2023.

⁵⁹ MENDES, Laura Schertel Ferreira. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014. p. 32.

⁶⁰ LESSIG, Lawrence. Reading the Constitution in Cyberspace. **Emory Law Journal**, v. 45, n. 3, p. 869-910, 1996.

⁶¹ Cf. CELLA, José Renato Gaziero; COPETTI, Rafael. Compartilhamento de dados pessoais e a Administração Pública brasileira. **Revista de Direito, Governança e Novas Tecnologias**, Maranhão, v. 3, n. 2, p. 39-58, 2017.

informações pessoais⁶².

Por conseguinte, a coleta e o repasse de dados, na seara tributária e nos demais setores da esfera pública, precisam respeitar a liberdade do indivíduo para “manter o controle sobre as próprias informações” e “determinar as modalidades de construção da própria esfera privada”⁶³. Nessa linha, ao se encorajar essa concepção voltada à proteção da autonomia do cidadão, a privacidade deve ser encarada como um bem comum, com especial relevância no Estado Democrático de Direito, pois assegura a participação deliberativa dos indivíduos. Desse modo, como aponta Bruno Bioni, isso beneficia não só o indivíduo, mas, também, a vida em sociedade⁶⁴.

A partir dessas diretrizes, observa-se que o objetivo da arrecadação tributária, ainda que legítimo e necessário para o bom funcionamento da máquina pública, não pode ser utilizado de forma desmedida pelas autoridades. As regras que regem esse propósito devem ser seguidas à risca e, principalmente, em estrita observância aos contornos acima definidos relativos à tutela da autodeterminação informativa.

1.3 Sigilo Fiscal

A consecução da atividade fiscalizadora, por inevitavelmente demandar a análise de informações pessoais dos contribuintes, deve pautar-se na proteção da privacidade e, como consequência, na inviolabilidade do sigilo de dados, garantias previstas na Constituição Federal de 1988 (art. 5º, incisos X e XII). Dessa forma, a Administração Tributária, como depositária do dever de guarda de informações econômicas e financeiras sensíveis, terá o sigilo fiscal como corolário a permitir a arrecadação de tributos e, concomitantemente, a proteção à intimidade.

Para que se possa definir os contornos do sigilo fiscal, é necessário analisar seu alcance e suas exceções na proteção constitucional da intimidade, da vida privada e do sigilo de dados, tanto para pessoas físicas como jurídicas⁶⁵.

Segundo o Manual Eletrônico do Sigilo Fiscal (e-MSF), elaborado pela Coordenação-Geral de Tributação da Receita Federal e aprovado pela Portaria RFB

⁶² SEER, 2020, p. 23.

⁶³ RODOTÀ, Stefano. **Tecnologie e diritti**. Bologna: il Mulino, 1995. p. 122.

⁶⁴ BIONI, Bruno. **Proteção de dados pessoais: a função e os limites do consentimento**. Rio de Janeiro: Forense, 2019. p. 216.

⁶⁵ ROCHA, Sergio André. **Troca de Informações para Fins Fiscais**. São Paulo: Quartier Latin, 2015. p. 149.

nº 4.820, de 19 de novembro de 2020⁶⁶, o sigilo fiscal, como desdobramento das garantias constitucionais à inviolabilidade da intimidade e da vida privada, é “a obrigação imposta à Fazenda Pública e a seus servidores de não divulgar 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”⁶⁷. Esse dever também está expressamente consignado no art. 198 CTN⁶⁸.

Desse modo, nos termos da redação conferida pela Receita Federal e pelo CTN, os dados fornecidos pelas pessoas físicas e jurídicas às Administrações Tributárias devem amparar o exercício das competências legais do órgão. O Fisco, contudo, possui vedação legal para facilitar de qualquer forma a divulgação dessas informações.

A Portaria RFB nº 2.344, de 24 de março de 2011, que regulamenta o acesso a informações protegidas por sigilo fiscal, constantes de sistemas informatizados da RFB, determina que “as informações sobre a situação econômica ou financeira do sujeito passivo ou de terceiros e sobre a natureza e o estado de seus negócios ou atividades, obtidas em razão do ofício para fins de arrecadação e fiscalização de tributos, inclusive aduaneiros”, são protegidas por sigilo fiscal (art. 2º)⁶⁹.

O dispositivo elenca, ainda, algumas das informações que estariam abrangidas pela definição dada pelo *caput*, quais sejam: aquelas concernentes a “rendas, rendimentos, patrimônio, débitos, créditos, dívidas e movimentação financeira ou patrimonial”; que “revelem negócios, contratos, relacionamentos

⁶⁶ BRASIL. Secretaria Especial da Receita Federal do Brasil. **Portaria RFB nº 4.820, de 19 de novembro de 2020**. Aprova o Manual Eletrônico do Sigilo Fiscal da Secretaria Especial da Receita Federal do Brasil (e-MSF). Boletim de Serviço da RFB, Brasília, DF, 23 nov. 2020, seção 1, p. 2. Disponível em: <http://normas.receita.fazenda.gov.br/sijut2consulta/link.action?naoPublicado=&idAto=113904&visao=anotado>. Acesso em: 24 fev. 2023.

⁶⁷ Disponível em: <https://www.gov.br/receitafederal/pt-br/assuntos/orientacao-tributaria/sigilo-fiscal/aspectos-gerais-sobre-o-sigilo-fiscal>. Acesso em: 27 fev. 2023.

⁶⁸ “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.”
BRASIL, 1966.

⁶⁹ BRASIL. Secretaria Especial da Receita Federal do Brasil. **Portaria RFB nº 2.344, de 24 de março de 2011**. Disciplina o acesso a informações protegidas por sigilo fiscal constantes de sistemas informatizados da Secretaria da Receita Federal do Brasil. Diário Oficial da União, Brasília, DF, 28 mar. 2011, seção 1, p. 33. Disponível em: <http://normas.receita.fazenda.gov.br/sijut2consulta/link.action?visao=anotado&idAto=30552>. Acesso em: 24 fev. 2023.

comerciais, fornecedores, clientes e volumes ou valores de compra e venda”; e as referentes a “projetos, processos industriais, fórmulas, composição e fatores de produção”⁷⁰.

O art. 6º da Portaria prevê que “[o] servidor que divulgar ou revelar informação protegida por sigilo fiscal, constante de sistemas informatizados, com infração ao disposto no art. 198 CTN, fica sujeito à penalidade de demissão prevista no art. 132, inciso IX, da Lei nº 8.112, de 1990”⁷¹. Além disso, ao sujeito passivo que se considerar prejudicado pelo uso indevido das informações previstas nesse ato normativo, é facultado dirigir representação à RFB para apuração do fato e, se for o caso, aplicação de penalidades cabíveis ao servidor responsável pela infração (art. 7º)⁷².

Para o tratamento das solicitações de fornecimento de dados econômico-fiscais de contribuintes recebidas pela RFB, foi editada a Portaria RFB nº 551, de 30 de abril de 2013, que estabelece as delimitações legais do sigilo fiscal para esses procedimentos. Segundo a norma, mesmo nas hipóteses em que a lei admitir o fornecimento das informações sigilosas pela RFB, essas não perdem o caráter sigiloso depois da sua entrega a órgãos, entidades e autoridades (art. 1º, § 2º)⁷³.

No entanto, vale lembrar que o sigilo fiscal não é absoluto, havendo exceções à regra previstas no próprio CTN. Segundo o § 1º do referido art. 198, excetuam-se do dever de sigilo a requisição de autoridade judiciária no interesse da justiça (inciso I) e as solicitações de autoridade administrativa no interesse do Poder Público, “desde que comprovada a instauração regular de processo administrativo, no órgão

⁷⁰ BRASIL, ref. 69.

⁷¹ “Art. 132. A demissão será aplicada nos seguintes casos:

[...]

IX - revelação de segredo do qual se apropriou em razão do cargo;”.

BRASIL. **Lei nº 8.112, de 11 de dezembro de 1990**. Dispõe sobre o regime jurídico dos servidores públicos civis da União, das autarquias e das fundações públicas federais. Brasília: Presidência da República, [1991]. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8112cons.htm. Acesso em: 24 fev. 2023.

⁷² BRASIL, ref. 69.

⁷³ BRASIL. Secretaria Especial da Receita Federal do Brasil. **Portaria RFB nº 551, de 30 de abril de 2013**. Dispõe sobre o tratamento de expedientes oriundos de outros órgãos, entidades, autoridades ou cidadãos utilizados para solicitar dados econômico-fiscais de contribuintes, análise de situação fiscal ou instauração de procedimento fiscal no âmbito da RFB, inclusive no que se refere à preservação do caráter sigiloso de informações protegidas por sigilo fiscal. BP/MF, Brasília, DF, 3 maio 2013. Disponível em: <http://normas.receita.fazenda.gov.br/sijut2consulta/link.action?visao=anotado&idAto=70296>. Acesso em: 24 fev. 2023.

ou na entidade respectiva, com o objetivo de investigar o sujeito passivo a que se refere a informação, por prática de infração administrativa” (inciso II)⁷⁴.

Demais disso, conforme dispõe o § 3º do art. 198, não há vedação para a divulgação de informações referentes a (i) representações fiscais para fins penais, (ii) inscrições na Dívida Ativa da Fazenda Pública e (iii) parcelamento ou moratória.

O já citado art. 199 do CTN, por sua vez, alberga a prestação de assistência mútua para a fiscalização de tributos e permuta de informações entre a Fazenda Pública da União e as dos Estados, do Distrito Federal e dos Municípios. O parágrafo único desse dispositivo também assegura a troca de informações com Estados estrangeiros na forma estabelecida em tratados, acordos ou convênios.

O § 1º do art. 2º da referida Portaria RFB nº 2.344, de 24 de março de 2011, também determina que não estão protegidas pela regra do sigilo as informações: (i) cadastrais do contribuinte, isto é, “as que permitam sua identificação e individualização” (v.g., nome, data de nascimento, endereço, filiação, qualificação e composição societária); (ii) relativas à regularidade fiscal do contribuinte, desde que não revelem valores de débitos ou créditos; (iii) agregadas⁷⁵, que não identifiquem o sujeito passivo; e (iv) previstas no já mencionado § 3º do art. 198 do CTN.

Vale lembrar, no entanto, que essas informações são protegidas por sigilo funcional, de forma que a sua divulgação por iniciativa de servidor da RFB configura violação ao art. 116, inciso VIII, da Lei nº 8.112, de 1990⁷⁶, segundo prescreve o § 2º do art. 2º desse ato normativo.

A flexibilização ou quebra do sigilo encontra fundamento no ordenamento. Conforme lecionam Schoueri e Barbosa, seria “razoável admitir a revelação de informações por parte da entidade que está obrigada a manter o sigilo, já que tal direito individual não deve ser utilizado como forma de proteção por aqueles que

⁷⁴ BRASIL, 1966.

⁷⁵ Segundo o art. 10 da Instrução Normativa SRF nº 19, de 17 de fevereiro de 1998, a RFB pode fornecer, mediante a celebração de convênio, dados econômico-fiscais às entidades que não detenham a competência para cobrar e fiscalizar tributos, desde que seja de forma agregada e não possibilite a identificação de contribuintes. Cf. BRASIL. Secretaria Especial da Receita Federal do Brasil. **Instrução Normativa SRF nº 19, de 17 de fevereiro de 1998**. Disciplina os procedimentos de fornecimento de dados cadastrais e econômico-fiscais da Secretaria da Receita Federal - SRF, a outras entidades. Diário Oficial da União, Brasília, DF, 18 fev. 1998, seção 1, p. 19. Disponível em: <http://normas.receita.fazenda.gov.br/sijut2consulta/link.action?visao=anotado&idAto=13242>. Acesso em: 24 fev. 2023.

⁷⁶ “Art. 116. São deveres do servidor:

[...]

VIII - guardar sigilo sobre assunto da repartição;”.

BRASIL, 1991.

violam a lei”⁷⁷. No entanto, a possibilidade de relativização a uma garantia constitucional deve vir acompanhada de uma justificativa adequada.

Em um primeiro momento, o Supremo Tribunal Federal (STF) “apontou o sigilo de dados como ‘regra’ a exigir que a exceção (a quebra do sigilo) fosse precedida da autorização do Judiciário”⁷⁸. Em 2010, ao apreciar o Recurso Extraordinário (RE) nº 389.808/PR, a Suprema Corte brasileira concluiu que viola o texto constitucional “norma legal atribuindo à Receita Federal – parte na relação jurídico-tributária – o afastamento do sigilo de dados relativo ao contribuinte”⁷⁹.

Naquele caso, discutia-se a constitucionalidade de determinação legal que facultava a utilização de dados relativos à Contribuição Provisória sobre Movimentação Financeira (CPMF) “para instaurar procedimento administrativo tendente a verificar a existência de crédito tributário relativo a impostos e contribuições e para lançamento, no âmbito do procedimento fiscal, do crédito tributário porventura existente”⁸⁰.

O STF concluiu, por maioria de votos, que deveria ser conferida interpretação conforme a Constituição a essa norma, “tendo como conflitante com esta a que implique afastamento do sigilo bancário do cidadão, da pessoa natural ou da jurídica, sem ordem emanada do Judiciário”⁸¹.

Prevaleceu a tese de que “ainda que o correntista goze da prerrogativa de ser julgado criminalmente pelo Supremo, este sim autorizado constitucionalmente a quebrar-lhe o sigilo de dados bancários, a Receita poderá fazê-lo não para efeitos criminais, mas de cobrança de tributos”, o que configuraria, na linha do voto

⁷⁷ SCHOUERI, Luís Eduardo; BARBOSA, Mateus Calicchio. Da antítese do sigilo à simplicidade do sistema tributário: desafios da transparência fiscal internacional. *In*: SANTI, Eurico Marcos Diniz; CHRISTOPOULOS, Basile Georges; ZUGMAN, Daniel Leib; BASTOS, Frederico Silva (Orgs.). **Transparência Fiscal e desenvolvimento**: homenagem ao Professor Isaías Coelho. São Paulo: FISCOsoft, 2013. p. 497-523. p. 507-508.

⁷⁸ MARQUES, Thiago de Mattos; LIOTTI, Belisa Ferreira. Troca de informações fiscais e o direito ao sigilo nas perspectivas doméstica e internacional: análise à luz dos requisitos fixados pelo STF nos precedentes de 2016. **Revista Direito Tributário Internacional Atual**, São Paulo, n. 9, ano 5, p. 177-212, 1º sem. 2021. p. 178.

⁷⁹ BRASIL. Supremo Tribunal Federal. **RE nº 389.808/PR**. Rel. Min. Marco Aurélio. Brasília, DF, Plenário, j. 15/12/2010, *DJ* 10/05/2011. Disponível em: <https://jurisprudencia.stf.jus.br/pages/search/sjur191883/false>. Acesso em: 6 out. 2023.

⁸⁰ BRASIL. **Lei nº 10.174, de 9 de janeiro de 2001**. Altera o art. 11 da Lei nº 9.311, de 24 de outubro de 1996, que institui a Contribuição Provisória sobre Movimentação ou Transmissão de Valores e de Crédito e Direitos de Natureza Financeira – CPMF, e dá outras providências. Brasília: Presidência da República, [2001]. Disponível em: https://www.planalto.gov.br/ccivil_03/Leis/LEIS_2001/L10174.htm. Acesso em: 24 fev. 2023.

⁸¹ BRASIL, ref. 79.

condutor do Ministro Marco Aurélio, verdadeira coação política na cobrança de tributos, a contrariar jurisprudência da Corte.

O Ministro Dias Toffoli, divergindo desse entendimento, havia destacado que a situação ventilada pela norma não se trataria de quebra de sigilo, mas, sim, de uma transferência de dados sigilosos de um portador desse dado que teria o dever de sigilo para um outro portador que também deveria observar essa obrigação. Pontuava, ainda, que, caso esse novo portador não mantivesse o sigilo, cometeria crime e seria responsabilizado.

Posteriormente, já em 2016, o Tribunal mudou seu posicionamento ao julgar o RE nº 601.314/SP⁸², Tema 225 da sistemática da repercussão geral. Aquele apelo extraordinário versava sobre a constitucionalidade do art. 6º da Lei Complementar nº 105/2001⁸³ frente ao parâmetro do sigilo bancário.

A referida norma autoriza que as autoridades e os agentes fiscais tributários da União, dos Estados, do Distrito Federal e dos Municípios examinem documentos, livros e registros de instituições financeiras, desde que haja processo administrativo instaurado ou procedimento fiscal em curso e tais exames sejam considerados indispensáveis pela autoridade competente.

Também se debatia se a utilização dos mecanismos fiscalizatórios previstos na já citada Lei nº 10.174/2001 ofenderia o princípio da irretroatividade das leis, quando empregados para a apuração de créditos relativos a tributos distintos da CPMF, cujos fatos geradores tenham ocorrido em período anterior à vigência desse diploma.

No sentido do voto do Ministro Edson Fachin, relator do feito, asseverou-se o caráter não absoluto da garantia de sigilo bancário ante as legítimas expectativas de obtenção de receitas públicas⁸⁴. Nessa linha, o Ministro destacou a tendência

⁸² BRASIL. Supremo Tribunal Federal. **RE nº 601.314/SP**. Rel. Min. Edson Fachin. Brasília, DF, Plenário, j. 24/2/2016, *DJ* 16/9/2016. Disponível em: <https://jurisprudencia.stf.jus.br/pages/search/sjur356216/false>. Acesso em: 6 out. 2023.

⁸³ "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." BRASIL. **Lei Complementar nº 105, de 10 de janeiro de 2001**. Dispõe sobre o sigilo das operações de instituições financeiras e dá outras providências. Brasília: Presidência da República, [2001]. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/lcp/lcp105.htm. Acesso em: 24 fev. 2023.

⁸⁴ BRASIL, ref. 82.

mundial, observada no Brasil, voltada à cooperação para as trocas de informações fiscais entre países, a exemplo da ratificação da *Convenção sobre Assistência Mútua Administrativa em Matéria Tributária*, das medidas no âmbito do projeto *Base Erosion and Profit Shifting (BEPS)*, da OCDE, e da adesão ao *Foreign Account Tax Compliance Act (FATCA)*, dos Estados Unidos⁸⁵.

Ademais, também se considerou que, à luz do princípio da igualdade tributária, o legislador estabeleceu requisitos objetivos para a requisição de informação pela Administração Tributária às instituições financeiras, bem como manteve o sigilo dos dados a respeito das transações financeiras do contribuinte. Nessa senda, destacou-se que o art. 6º da Lei Complementar nº 105/2001 é taxativo ao possibilitar o acesso a documentos, livros e registros de instituições financeiras, apenas se (i) houver processo administrativo instaurado ou procedimento fiscal em curso e (ii) tais exames sejam considerados indispensáveis pela autoridade competente.

No que atine à Lei nº 10.174/2001, o voto do relator, reputando a norma como de caráter meramente instrumental (art. 144, § 1º, do CTN), foi no sentido da não aplicação do princípio da irretroatividade das leis tributárias. Isso porque não se evidenciou, segundo esse posicionamento, alteração na ordem jurídica promovida pelo referido diploma, mas apenas se instituiu uma regra que “se encerra na atribuição de competência administrativa à Secretaria da Receita Federal”, isto é, uma alteração legislativa que tem somente o condão de aprimorar a atividade fiscalizatória dos órgãos da RFB.

Essa conclusão quanto à validade do texto legal partiu da compreensão de que a lei em referência não estabelece nova hipótese de incidência para o tributo ou cria qualquer obrigação tributária principal. Nesse sentido, verifica-se que houve uma nova leitura quanto à inviolabilidade da privacidade, com base na ideia de ampliação dos poderes de fiscalização da Administração Pública.

Por conseguinte, a Corte fixou as seguintes teses⁸⁶:

⁸⁵ Cf. ESTADOS UNIDOS. U.S. Department of the Treasury. **Agreement between the Government of the United States of America and the Government of the Federative Republic of Brazil to Improve International Tax Compliance and to Implement FATCA**. Disponível em: <https://home.treasury.gov/system/files/131/FATCA-Agreement-Brazil-9-23-2014.pdf>. Acesso em: 20 maio 2023.

⁸⁶ BRASIL, ref. 82.

I - 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;
II - A Lei 10.174/01 não atrai a aplicação do princípio da irretroatividade das leis tributárias, tendo em vista o caráter instrumental da norma, nos termos do artigo 144, § 1º, do CTN.

Nessa mesma assentada, o STF apreciou a Ação Direta de Inconstitucionalidade (ADI) nº 2.859⁸⁷, julgada em conjunto com as ADIs nº 2.386, nº 2.390 e nº 2.397.

Naquelas ações, eram impugnadas diversas normas federais relativas ao fornecimento, pelas instituições financeiras, de informações bancárias de correntistas à Administração Tributária. No sentido da supracitada repercussão geral, o STF entendeu que os dispositivos analisados “consagram, de modo expresso, a permanência do sigilo das informações bancárias obtidas com espreque em seus comandos, não havendo neles autorização para a exposição ou circulação daqueles dados”⁸⁸.

No aresto, restou consignado que o dever fundamental de pagar tributos é essencial à ordem constitucional instaurada em 1988, eis que assim se viabiliza o financiamento de ações estatais voltadas à concretização dos direitos dos cidadãos. Nessa toada, o instrumento fiscalizatório instituído pelas normas impugnadas opera como mecanismo efetivo de combate à sonegação fiscal e, dessa forma, como meio para se alcançar os objetivos da República Federativa do Brasil.

Esses dois casos paradigmáticos de 2016 demonstram que, ante a coexistência dos direitos à privacidade e ao sigilo de dados, uma situação de colisão entre eles permitiria a conclusão da Corte, em consonância com os compromissos firmados pelo Brasil no plano internacional, no sentido da possibilidade de transmissão de dados, desde que respeitada a manutenção da confidencialidade. Trata-se, no caso, de leitura dos incisos X e XII do art. 5º da Constituição Federal como regras constitucionais que devem ser submetidas a um processo de ponderação e, portanto, não são absolutamente inafastáveis.

Esse exame perpassa, invariavelmente, pelo postulado da proporcionalidade: com o confronto entre regras constitucionais, deve-se fazer a avaliação de

⁸⁷ BRASIL. Supremo Tribunal Federal. **ADI nº 2.859**. Rel. Min. Dias Toffoli. Brasília, DF, Plenário, j. 24/2/2016, *DJ* 21/10/2016. Disponível em: <https://jurisprudencia.stf.jus.br/pages/search/sjur358417/false>. Acesso em: 6 out. 2023.

⁸⁸ BRASIL, ref. 87, p. 2.

adequação e necessidade na operação de transmissão de dados dos contribuintes para as autoridades fiscais com o objetivo de se combater a sonegação, mas sem perder de vista os direitos à privacidade e ao sigilo de dados. O juízo de necessidade revela-se claro, eis que a transmissão de dados bancários ao Fisco é inquestionavelmente apta à promoção da finalidade de se combater a sonegação fiscal. Sobre o exame de adequação, Belisa Liotti e Thiago Marques explicam o seguinte⁸⁹:

Uma vez que alcançar determinado fim não justifica o recurso a quaisquer meios, poder-se-ia sugerir a desnecessidade da transmissão automática de dados à fiscalização tributária, por exemplo, ao argumento de que a transferência poderia ser precedida da autorização do Judiciário, o que resultaria em menor restrição aos direitos à privacidade e ao sigilo de dados. Todavia, no caso concreto, tal argumento não parece proceder porque a ordem dos fatores ('transmissão de dados' e 'fiscalização') altera o resultado ('combate à sonegação'), já que o acesso automático às informações bancárias de empresas e indivíduos é utilizado pelas autoridades fiscais justamente para identificar quais contribuintes movimentam valores que não são condizentes com a renda (ou receita) declarada, iniciando a cabível fiscalização. Sem o acesso automático, o Fisco não teria conhecimento de informações que permitem identificar situações suspeitas que podem revelar casos de sonegação. Isso impede que essa modalidade de transmissão de dados seja considerada como manifestamente menos adequada do que a transmissão dependente de autorização judicial.

Nessa perspectiva, ainda que uma eventual imposição de regra que demandasse prévia autorização judicial para acessar os dados pudesse resultar em uma menor restrição aos direitos à privacidade e ao sigilo de dados, é justamente o acesso automático às informações bancárias de empresas e de indivíduos que permite a identificação, pelas autoridades fiscais, dos contribuintes que movimentam valores não condizentes com o montante declarado. Assim, a instauração da fiscalização cabível só é viabilizada em razão da possibilidade de o Fisco se antecipar e identificar essas situações suspeitas.

Por fim, considerando-se a proporcionalidade em sentido estrito, nota-se que um fator predominante no entendimento da Corte quanto à validade das normas foi: resguardar o sigilo dos dados após a transmissão ao Fisco. É dizer: mesmo que as informações guardadas pelas instituições financeiras fossem repassadas, as autoridades fiscais deveriam manter esse dever de sigilo.

⁸⁹ MARQUES; LIOTTI, 2021, p. 193-194.

Tanto é assim que, no julgamento da ADI nº 2.859, o Supremo fez expressa ressalva em relação aos Estados e Municípios no sentido de que esses entes somente poderão obter as informações de que trata o art. 6º da Lei Complementar nº 105/2001 quando a matéria estiver devidamente regulamentada, observando os seguintes requisitos para a manutenção de sigilo de dados, indicados no voto do Ministro Dias Toffoli⁹⁰:

- i) pertinência temática entre as informações bancárias requeridas na forma do art. 6º da LC nº 105/01 e o tributo objeto de cobrança no processo administrativo instaurado;
- ii) prévia notificação do contribuinte quanto à instauração do processo (leia-se, o contribuinte deverá ser notificado da existência do processo administrativo previamente à requisição das informações sobre sua movimentação financeira) e relativamente a todos os demais atos;
- iii) submissão do pedido de acesso a um superior hierárquico do agente fiscal requerente;
- iv) existência de sistemas eletrônicos de segurança que sejam certificados e com registro de acesso, de modo que torne possível identificar as pessoas que tiverem acesso aos dados sigilosos, inclusive para efeito de responsabilização na hipótese de abusos;
- v) estabelecimento de mecanismos efetivos de apuração e correção de desvios;
- vi) amplo acesso do contribuinte aos autos, garantindo-lhe a extração de cópias de quaisquer documentos e decisões, de maneira a permitir que possa exercer a todo tempo o controle jurisdicional dos atos da administração, segundo atualmente dispõe a Lei 9.784/1999.

Nessa linha, no julgamento do RE nº 1.055.941/SP⁹¹, representativo do Tema 990 da sistemática da repercussão geral, a Corte analisou a possibilidade de a Receita Federal, no legítimo exercício de seu dever de fiscalizar, compartilhar dados bancários e fiscais com o Ministério Público para fins penais.

Na oportunidade, discutia-se se o compartilhamento dos dados obtidos pela RFB com o Ministério Público afrontaria os direitos fundamentais à privacidade e à inviolabilidade do sigilo de dados. Caso o fornecimento fosse considerado inválido, as provas obtidas por meio dessa divulgação entre órgãos seriam ilícitas.

Todavia, restou assentada a tese no sentido da constitucionalidade do compartilhamento da íntegra do procedimento fiscalizatório da RFB com os órgãos de persecução penal para fins criminais, sem a obrigatoriedade de prévia autorização judicial. Na conclusão da Corte, também se determinou que esse

⁹⁰ BRASIL, ref. 87, p. 33-34.

⁹¹ BRASIL. Supremo Tribunal Federal. **RE nº 1.055.941/SP**. Rel. Min. Dias Toffoli. Brasília, DF, Plenário, j. 4/12/2019, DJ 18/3/2021. Disponível em: <https://jurisprudencia.stf.jus.br/pages/search/sjur433179/false>. Acesso em: 6 out. 2023.

compartilhamento “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”⁹².

O entendimento do STF levou em consideração a jurisprudência firmada pelo tribunal em matéria de sigilo fiscal. O Ministro Dias Toffoli, relator do caso, em seu voto, ressaltou que o tribunal “elevou o sigilo fiscal (ao lado do sigilo bancário e do sigilo telefônico) à categoria de direito fundamental, por entender que ele representa projeção específica dos direitos à intimidade e à inviolabilidade de dados”⁹³, e, por conta disso, deveria prevalecer a necessidade de prévia autorização judicial para a quebra do sigilo.

Também merece destaque, no bojo dos julgamentos do STF sobre a matéria, a ADI nº 5.729⁹⁴, que discutia a validade da Lei nº 13.254, de 13 de janeiro de 2016 (“Lei da Repatriação”)⁹⁵, a qual dispõe sobre o Regime Especial de Regularização Cambial e Tributária (RERCT) de recursos, bens ou direitos de origem lícita, não declarados ou declarados incorretamente, remetidos, mantidos no exterior ou repatriados por residentes ou domiciliados no País.

O referido diploma legal equipara a divulgação ou a publicidade das informações presentes no RERCT à quebra do sigilo fiscal, sujeitando o responsável às mesmas penas previstas na legislação sobre essa matéria, e, no caso de funcionário público, à pena de demissão (art. 7º, § 1º). A lei ainda veda à RFB, ao Conselho Monetário Nacional (CMN), ao Banco Central do Brasil (BACEN) e aos demais órgãos públicos envolvidos no RERCT o compartilhamento das informações prestadas pelos declarantes que aderirem ao regime com os Entes Federativos, “inclusive para fins de constituição de crédito tributário” (art. 7º, § 2º).

No caso, alegava-se a violação constitucional pelos dispositivos em razão de o art. 37, inciso XXII, da Lei Maior prever o dever de troca de informações entre as Administrações Tributárias da União, dos Estados, do Distrito Federal e dos

⁹² BRASIL, ref. 91, p. 2.

⁹³ BRASIL, ref. 91, p. 72.

⁹⁴ BRASIL. Supremo Tribunal Federal. **ADI nº 5.729**. Rel. Min. Roberto Barroso. Brasília, DF, Plenário, j. 8/3/2021, DJ 17/3/2021. Disponível em: <https://jurisprudencia.stf.jus.br/pages/search/sjur442417/false>. Acesso em: 6 out. 2023.

⁹⁵ BRASIL. **Lei nº 13.254, de 13 de janeiro de 2016**. Dispõe sobre o Regime Especial de Regularização Cambial e Tributária (RERCT) de recursos, bens ou direitos de origem lícita, não declarados ou declarados incorretamente, remetidos, mantidos no exterior ou repatriados por residentes ou domiciliados no País. Brasília: Presidência da República, [2016]. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2016/Lei/113254.htm. Acesso em: 24 fev. 2023.

Municípios. Contudo, o STF concluiu, nos termos do voto do relator, Ministro Roberto Barroso, que “toda a tributação incidente sobre esses recursos se encerra no âmbito do próprio programa, cujo desenvolvimento é atribuído exclusivamente à Receita Federal do Brasil”⁹⁶. Dessa maneira, entenderam os Ministros que não haveria interesse no compartilhamento com as demais Administrações Tributárias.

Além disso, em seu voto, o Ministro Barroso lembrou que o compartilhamento de dados não seria uma regra absoluta e que, ao vedar essa prática no âmbito do RERCT, o legislador nada mais fez do que criar “uma restrição pontual e específica, dentro de sua margem de conformação jurídica”⁹⁷.

Nesse julgamento, o STF buscou demonstrar o total alinhamento da sua orientação com as boas práticas previstas nos relatórios e estudos da OCDE. Inclusive, é citado, no acórdão, o relatório “*Update on voluntary disclosure programmes: a pathway to tax compliance*”, elaborado em 2015 pela organização⁹⁸. No documento, destaca-se que a confidencialidade precisa estar baseada nas obrigações e leis em vigor no país, devendo, ainda, ser explicada de forma clara aos contribuintes. Também é defendido que, na medida do possível, deve haver transparência quanto ao uso dos dados coletados por meio do processo voluntário de *disclosure* e compartilhamento entre entidades governamentais. Afinal, um dos pilares mais importantes da organização, a fim de eliminar planejamentos tributários abusivos em seus países-membros, é o aprimoramento da troca de informações com base em acordos multilaterais firmados pelas diferentes Administrações Tributárias⁹⁹.

⁹⁶ BRASIL, ref. 94, p. 16.

⁹⁷ BRASIL, ref. 94, p. 16.

⁹⁸ OCDE. **Update on Voluntary Disclosure Programmes**: A pathway to tax compliance. Paris: OECD Publishing, 2015, p. 24. Disponível em: <https://www.oecd.org/ctp/exchange-of-tax-information/update-on-voluntary-disclosure-programmes-a-pathwayto-tax-compliance.htm>. Acesso em: 24 fev. 2023.

⁹⁹ Nesse sentido, os últimos relatórios da organização têm demonstrado resultados satisfatórios na troca de informações entre países: “O desempenho das ‘jurisdições’ no padrão EOIR [*Exchange Information on Request*] continua forte, com 86% das jurisdições analisadas na segunda rodada tendo recebido uma classificação geral satisfatória (‘Em conformidade’ ou ‘Amplamente em conformidade’). Quase metade dos membros do Fórum Global já foi analisada nessa rodada, incluindo 20 deles em 2020. As jurisdições sujeitas a um monitoramento anual de acompanhamento informaram que mais de 90% das mais de 550 recomendações foram ‘atendidas’ ou ‘estão em processo de atendimento’” (tradução nossa). OCDE. **Tax Transparency and Exchange of Information in Times of COVID-19**: 2020 Global Forum Annual Report. Paris: OECD Publishing, 2020, p. 18. Disponível em: <https://www.oecd.org/tax/transparency/documents/global-forum-annual-report-2020.pdf>. Acesso em: 24 fev. 2023.

Como visto, o sigilo fiscal comporta diferentes nuances e pode ser relativizado, desde que observadas as garantias constitucionais de proteção à privacidade e de inviolabilidade do sigilo de dados do contribuinte. Assim, para que se tenham bem definidas as suas balizas, é importante analisar, também, quais dados podem ser compartilhados e em que medida estão amparados pelo direito à privacidade, bem como quais seriam as normas que regulamentam a divulgação e o grau de detalhamento dessas informações.

Para essa tarefa, é imprescindível que não se perca de vista a necessidade de que a flexibilização da regra de sigilo acompanhe a ressignificação que se tem dado às informações pessoais a partir dos avanços tecnológicos. O Fisco, como detentor de uma extensa base de dados, deve sempre estar atento a essas mudanças.

1.4 Considerações sobre a aplicabilidade do direito à privacidade à luz do sigilo fiscal

Da análise dos aludidos julgados e normas, é possível concluir que, no âmbito do direito tributário, o direito à privacidade comporta alguns desafios intrínsecos às especificidades da matéria. Mesmo que o intercâmbio de informações busque refletir um aparente equilíbrio de direitos – privacidade dos contribuintes, por um lado, e, por outro, a obtenção de informações necessárias pelas autoridades fiscais – a intensificação da coleta e do compartilhamento aumentou as preocupações com as garantias individuais.

Essas inquietações partem de uma leitura das operações tributárias que vai além do sigilo fiscal e compreende, ainda, o ideal de privacidade de cada contribuinte.

Isso também repercute no cenário global, em que foram formados verdadeiros “*Big Datas*” tributários com dados agregados dos contribuintes, o que levanta uma série de questionamentos; tais como: (i) se as informações transferidas estão tão bem protegidas pelas leis do país destinatário quanto pelas leis do país remetente¹⁰⁰; (ii) se há o risco de os dados serem utilizados indevidamente pelo

¹⁰⁰ A respeito do tema, Cf. LIMA, Juciléia. Proteção de Dados dos Contribuintes na Troca de Informações Fiscais. **Revista Direito Tributário Atual**, São Paulo, n. 38, p. 34-52, 2017.

destinatário para fins políticos e/ou econômicos; (iii) se as informações podem ser usadas de forma incorreta para sancionar contribuintes por motivos políticos; (iv) se as bases podem ser acessadas ou alteradas ilegalmente por terceiros; ou (v) se as comunicações podem ser fraudadas ou imprecisas¹⁰¹.

As informações de um contribuinte, como bem pontua Arthur J. Cockfield, são consideradas “uma das formas mais sensíveis de informações pessoais”, eis que podem revelar, entre outros aspectos, dados sobre renda, gastos, pertences pessoais, incapacidade, associações e afiliações, doações, financiamentos e empréstimos, pensões etc. Assim, qualquer autoridade ou terceiro munido dessas informações detalhadas pode utilizá-las para “construir um perfil abrangente da identidade de um indivíduo, incluindo suas crenças religiosas, alianças políticas e comportamento pessoal”¹⁰².

Tais preocupações podem ser trazidas para a realidade brasileira, especialmente porque, conforme será explorado nos próximos capítulos, algumas das normas internas sobre o tema ainda são genéricas e abertas, o que pode resultar em um conflito com as regras internacionais mais restritivas. Todavia, diante desse conflito, o art. 98 do Código Tributário Nacional prevê a solução: “[o]s tratados e as convenções internacionais revogam ou modificam a legislação tributária interna, e serão observados pela que lhes sobrevenha”¹⁰³. Portanto, considerando a especificidade das normas internacionais, medidas mais estritas de confidencialidade deveriam, sob esse prisma, prevalecer no direito interno.

De todo modo, é importante que o debate seja orientado por uma visão ponderada da relação entre a atividade estatal e o direito à privacidade. Sobre esse ponto, Daniel J. Solove tece algumas considerações em relação à falsa impressão de que haveria um *tradeoff* entre as liberdades individuais e o dever de segurança conferido à Administração Pública.

Segundo o autor, “a privacidade geralmente perde para a segurança quando não devia”, porque, enquanto há uma certa facilidade para se compreender os interesses da segurança na atividade estatal – uma vez que a vida e a integridade

Disponível em: <https://revista.ibdt.org.br/index.php/RDTA/article/view/332/649>. Acesso em: 10 maio 2023.

¹⁰¹ COCKFIELD, 2020, p. 3.

¹⁰² COCKFIELD, Arthur J. Big Data and Tax Haven Secrecy. **Florida Tax Review**, v. 18, p. 483-539, 2016. p. 503. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2757268. Acesso em: 20 maio 2023.

¹⁰³ BRASIL, 1966.

física do cidadão estão em jogo –, os direitos inerentes à privacidade são abstratos e vagos, o que os torna de difícil materialização no plano fático¹⁰⁴.

Isso faz com que se crie a crença, enraizada no imaginário da população, de que seria necessário renunciar à privacidade para estar mais seguro. Essa percepção, por estar pautada na ideia de segurança, traz consigo fortes argumentos para que as pessoas acabem aceitando o *tradeoff*. Essa tendência é fortalecida pelo argumento do “nada a esconder” (*nothing-to-hide argument*). Trata-se de expressão que, ao passo que diminui o conceito de privacidade, também incentiva a prática de monitoramento a todo custo. Para contrapor esse raciocínio, Solove menciona a história narrada em “O Processo”, de Franz Kafka.

No romance, um homem é preso sem ser informado o motivo e tenta desesperadamente descobrir quais seriam as suas acusações. Mas, ao descobrir a existência de um sistema judicial secreto, que possuiria um dossiê sobre ele, o personagem não consegue obter mais informações sobre a investigação. O caso se desenvolve a partir do embate entre o uso da máquina estatal para a tomada de decisões com base em informações pessoais e a negativa de participação dos cidadãos envolvidos, que sequer podem ter ciência dos dados que são utilizados.

Segundo Daniel Solove, os problemas retratados pela metáfora kafkiana vão além dos desafios da vigilância¹⁰⁵:

Em vez disso, são problemas de processamento de informações – armazenamento, uso ou análise de dados – e não de coleta de informações. Eles afetam as relações de poder entre as pessoas e as instituições do Estado moderno. Eles não apenas frustram o indivíduo ao criar uma sensação de desamparo e impotência, mas também afetam a estrutura social ao alterar o tipo de relacionamento que as pessoas têm com as instituições que tomam decisões importantes sobre suas vidas (tradução nossa).

Com base nesse exemplo, o autor observa que os defensores do argumento do “nada a esconder” apontam apenas situações em que as pessoas de fato querem esconder informações. Ocorre que, com isso, se cria a suposição de que a

¹⁰⁴ SOLOVE, Daniel J. **Nothing to hide**: the false tradeoff between privacy and security. New Haven: Yale University Press, 2011. p. 2.

¹⁰⁵ No original: “*Instead, they are problems of information processing – the storage, use, or analysis of data – rather than of information collection. They affect the power relationships between people and the institutions of the modern state. They not only frustrate the individual by creating a sense of helplessness and powerlessness, they also affect social structure by altering the kind of relationships people have with the institutions that make important decisions about their lives*”. SOLOVE, 2011, p. 26.

privacidade tem a ver com ocultar “coisas ruins”.

A privacidade, no entanto, precisa ser considerada com base na pluralidade de significados que o instituto comporta. Dessa forma, a revelação de “coisas ruins” é “apenas uma entre muitas dificuldades causadas pelas medidas de segurança do governo”. Assim como se constatou no romance kafkiano, há também danos burocráticos: “a impotência e a vulnerabilidade sufocantes criadas pelo uso de dados pessoais pelo sistema judiciário e a negação ao protagonista de qualquer conhecimento ou participação no processo”¹⁰⁶.

Diante de tais considerações, conclui-se que, sob essa mesma perspectiva, a garantia da segurança dos procedimentos envolvidos na tributação não pode significar uma necessária abdicação da privacidade. O argumento de “nada a esconder” também não pode ser um trunfo nas relações jurídico-tributárias, notadamente quando se pretender valer-se do dever de sigilo contra o titular dos dados para assegurar a eficiência da fiscalização, em detrimento dos direitos individuais de personalidade.

¹⁰⁶ SOLOVE, 2011, p. 27.

CAPÍTULO II

O ARCABOUÇO NORMATIVO BRASILEIRO SOBRE A COLETA, TRANSMISSÃO E PROTEÇÃO DE DADOS DOS CONTRIBUINTES

“A norma não existe, não é ‘aplicável’. Ela é produzida apenas no processo de concretização. O operador do direito se vê incluído nesse processo de construção de normatividade, normativa e materialmente vinculada, da mesma maneira como a estrutura do problema do caso ou do tipo de caso.”

(Friedrich Müller)¹⁰⁷

2.1 Considerações preliminares

A Administração Tributária, como não poderia deixar de ser, sempre buscará maximizar o cumprimento das obrigações tributárias, a fim de (i) garantir a equidade do sistema, sob uma perspectiva de justiça econômica e distributiva, bem como (ii) não privilegiar o inadimplente¹⁰⁸. Da mesma forma, a busca por eficiência produz efeitos positivos diretos na sociedade, eis que o cidadão é o principal beneficiário dessa atividade exercida pelo Estado. Nas lições de Marçal Justen Filho, “[é] o bem-estar do cidadão que justifica a existência do sistema tributário”¹⁰⁹.

¹⁰⁷ MÜLLER, Friedrich. **Teoria Estruturante do Direito**. Tradução de Peter Naumann e Eurides Avance de Souza. São Paulo: Revista dos Tribunais, 2008. p. 80.

¹⁰⁸ VIOL, Andrea Lemgruber. A Administração Tributária moderna e a maximização do cumprimento tributário: algumas reflexões sobre o caso brasileiro. **Revista da Receita Federal: estudos tributários e aduaneiros**, Brasília, v. 1, n. 2, p. 50-82, jan./jul. 2015. p. 50. Disponível em: <https://www.gov.br/receitafederal/pt-br/centrais-de-conteudo/publicacoes/revistas/revista-da-receita-federal/2015-revista-de-estudos-tributarios-e-aduaneiros-da-receita-federal-1.pdf/view>. Acesso em: 20 maio 2023; MURPHY, Liam; NAGEL, Thomas. **O Mito da propriedade: os impostos e a justiça**. Tradução de Marcelo Brandão Cipolla. São Paulo: Martins Fontes, 2005. p. 5.

¹⁰⁹ JUSTEN FILHO, Marçal. Sistema constitucional tributário: uma aproximação ideológica. **Revista da Faculdade de Direito da UFPR**, Curitiba, a. 30, n. 30, p. 215-233, 1998. p. 221. Disponível em: <https://revistas.ufpr.br/direito/article/view/1894/1589>. Acesso em: 20 maio 2023.

Nesse sentido, para que se possa alcançar tal eficiência, é imprescindível que a atividade de fiscalização tributária seja subsidiada por informações precisas e confiáveis. Afinal, o exame de subsunção à norma tributária exige minuciosa análise das operações dos contribuintes.

Com o desenvolvimento do papel da tecnologia nos processos de governança pública, viu-se uma transição do conceito de Governo Eletrônico para o conceito de Governo Digital¹¹⁰. Nesse cenário, as tecnologias digitais assumem papel fundamental nas estratégias de modernização do Estado¹¹¹ e, com isso, torna-se crucial o amplo acesso a dados econômicos e financeiros para a consecução da atuação estatal.

O fornecimento de dados para auxiliar essa atividade decorre da proeminência da Administração Tributária em razão da sua competência para fiscalizar e cobrar tributos. Nesse particular, o desenvolvimento tecnológico inevitavelmente facilitou a produção, edição, disseminação e o armazenamento de todas as informações e, assim, permitiu uma fiscalização mais prática e eficiente¹¹². Por exemplo, no âmbito federal, para que a RFB possa verificar o cumprimento das obrigações atinentes ao Imposto de Renda (IR), são fornecidas diversas informações pelas declarações digitais de ajuste anual, a exemplo dos informes de rendimentos e dos bens e direitos pertencentes ao contribuinte¹¹³. Juntamente com essas informações declaradas pelo próprio contribuinte, são cruzados os dados fornecidos por empresas, instituições financeiras, planos de saúde etc.

Por outro lado, para que se analise o adimplemento da Contribuição para o Programa de Integração Social (PIS) e da Contribuição para o Financiamento da Seguridade Social (COFINS), o Fisco pode obter acesso aos livros eletrônicos e aos arquivos contábeis e fiscais, de forma a investigar quaisquer irregularidades na apuração do faturamento da empresa. Já para o Imposto sobre Operações Financeiras (IOF), a fiscalização poderá proceder à análise da relação de transações financeiras realizadas pelo contribuinte, tributáveis e isentas, e das informações bancárias, como a relação mensal dos empréstimos em conta.

¹¹⁰ Cf. OCDE. **Recommendation of the Council on Digital Government Strategies**. Paris: OECD Publishing, 2014. Disponível em: <https://www.oecd.org/gov/digital-government/recommendation-on-digital-government-strategies.htm>. Acesso em: 20 maio 2023.

¹¹¹ WIMMER, 2021, p. 274.

¹¹² A propósito: WÖHRER, Victoria. **Data Protection and Taxpayers' Rights: Challenges Created by Automatic Exchange of Information**. Amsterdam: IBFD, 2018. p. 2-3.

¹¹³ Disponível em: <https://www.gov.br/receitafederal/pt-br/assuntos/meu-imposto-de-renda>. Acesso em: 27 fev. 2023.

Como se vê, há uma miríade de instrumentos voltados para a atividade fiscalizadora, que são fortemente subsidiados por dados pessoais. Neste capítulo, inicialmente, são examinadas algumas das principais regras tributárias vigentes sobre a troca de informações para, em seguida, discorrer sobre as normas de proteção de dados que circundam o tema deste trabalho. Ao final, investiga-se a aplicabilidade dos comandos legais e constitucionais de proteção de dados pessoais à seara tributária.

2.2 O processo de coleta e transmissão de informações pelo Fisco

O fornecimento de informações ao Fisco pode se dar *ex ante* e *ex post*. Em um primeiro momento (*ex ante*), as autoridades fiscais podem exigir que os contribuintes disponibilizem uma série de dados atinentes a pagamentos, transações, eventos etc. Além disso, terceiros que fazem negócios ou prestam serviços a esses contribuintes também são obrigados a fornecer subsídios para complementar e validar as informações autodeclaradas. Como bem explica Steven A. Dean, a troca desses dados serve a dois propósitos interligados: (i) desestimular afirmativamente a inadimplência (*noncompliance*) e (ii) permitir que as autoridades identifiquem a inadimplência¹¹⁴.

Exemplo disso é a obrigação de os empregadores e as instituições financeiras fornecerem informações sobre os rendimentos de seus empregados e investidores, respectivamente. Dean assinala que, quando elementos dessa natureza não são disponibilizados por intermediários, a autodeclaração se torna muito menos confiável¹¹⁵:

Por um lado, se os contribuintes acreditam que o governo foi notificado de que eles receberam pagamentos que quase certamente representam itens de renda tributável, os contribuintes têm pouco a ganhar deixando de

¹¹⁴ DEAN, Steven A. The incomplete global market for tax information. **Boston College Law Review**, v. 49, n. 605, p. 605-672, 2008. p. 620. Disponível em: <https://brooklynworks.brooklaw.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1434&context=faculty>. Acesso em: 24 fev. 2023.

¹¹⁵ No original: “On the one hand, if taxpayers believe that the government has been notified that they have received payments that almost certainly represent items of taxable income, taxpayers have little to gain by failing to report those amounts. On the other hand, a taxpayer confident that the government has no way of knowing that she has received income may only have her conscience to contend with if she fails to report it. As a result, by encouraging compliance, *ex ante* information reporting requirements not only help authorities to correct taxpayer omissions but also limit the need to make such corrections”. DEAN, 2008, p. 620-621.

declarar esses valores. Por outro lado, um contribuinte confiante de que o governo não tem como saber que ele recebeu renda pode ter apenas que lidar com sua consciência se não a declarar. Como resultado, ao incentivar a conformidade, as exigências de relatórios contendo informações *ex ante* não apenas ajudam as autoridades a corrigir as omissões dos contribuintes, mas também limitam a necessidade de se fazer tais correções (tradução nossa).

A despeito dos esforços das autoridades tributárias, tanto a subnotificação quanto a fraude fiscal são desafios que podem tornar a fiscalização *ex ante* insuficiente. Dessa maneira, a fim de enfrentar essas questões, o Fisco também dispõe de um poder de polícia para coletar informações *ex post*, que permite, dentro dos limites legalmente impostos, que sejam requisitados dados voltados a subsidiar os procedimentos fiscais¹¹⁶.

Nessa linha de ideias, os Entes Federativos brasileiros contam com uma extensa – e esparsa – legislação tributária sobre essas duas formas de fiscalização. Neste trabalho, serão analisadas, principalmente, as normas federais sobre os processos de coleta e de transmissão de dados. Isso porque os dados que se relacionam com as informações fiscais para a apuração e a cobrança de tributos de competência da União, como o IR ou mesmo as contribuições sociais PIS e COFINS, têm relação direta com dados pessoais de contribuintes.

Trata-se, nesse sentido, de exações que são apuradas conforme informações precisas sobre, *e.g.*, patrimônio, rendimento, faturamento, operações com ativos etc. Desse modo, será explorada, a partir de alguns exemplos relevantes, a forma pela qual o Fisco federal tem fixado suas regras procedimentais em relação a esses dados.

2.2.1 Decreto nº 10.046/2019

Popularmente conhecido como “Cadastrão”, o Decreto nº 10.046, de 9 de outubro de 2019¹¹⁷, fixou “normas e diretrizes para o compartilhamento de dados entre os órgãos e as entidades da administração pública federal direta, autárquica e fundacional e os demais Poderes da União”. O diploma legal decorre de uma

¹¹⁶ DEAN, 2008, p. 621-622.

¹¹⁷ BRASIL. **Decreto nº 10.046, de 9 de outubro de 2019**. Dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados. Brasília: Presidência da República, [2019]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D10046.htm. Acesso em: 13 mar. 2023.

evolução dos debates legislativos em relação ao Decreto nº 8.789, de 29 de junho de 2016¹¹⁸, que buscou inicialmente disciplinar a matéria. Essa primeira regulamentação recebeu duras críticas por parte da doutrina, em razão da excessiva vagueza na abordagem do tema. Isso porque a norma anterior não impunha “limites expressos à extensão do cruzamento de dados entre variados órgãos e entidades do Estado e a classificação das informações que podem ser obtidas”¹¹⁹.

O Decreto nº 10.046/2019 elenca as finalidades da Administração com o uso de dados; quais sejam: (i) simplificação da oferta de serviços públicos; (ii) viabilização da análise das condições de acesso e manutenção de benefícios sociais e fiscais; (iii) orientação e otimização da formulação, da implementação, da avaliação e do monitoramento de políticas públicas; (iv) promoção da melhoria da qualidade e da confiabilidade dos dados custodiados pela Administração Pública federal; e (v) aumento da qualidade e da eficiência das operações internas da Administração Pública federal (art. 1º, incisos I a V).

Apesar de a norma excluir a aplicação de tais diretrizes aos dados protegidos por sigilo fiscal sob gestão da Secretaria Especial da Receita Federal do Brasil, conforme delineado em seu art. 1º, § 2º, possibilita-se o compartilhamento de diversos dados cadastrais, que são definidos, de forma exemplificativa, no art. 2º, inciso III, da norma¹²⁰.

Em relação aos dados não sigilosos, há previsão expressa no sentido de a RFB e a Procuradoria-Geral da Fazenda Nacional (PGFN) compartilharem as seguintes informações (arts. 28 e 29)¹²¹:

Art. 28. A Secretaria Especial da Receita Federal do Brasil do Ministério da Fazenda disponibilizará aos órgãos interessados os seguintes dados não protegidos por sigilo fiscal:
I - informações constantes da declaração de operações imobiliárias relativas

¹¹⁸ BRASIL. **Decreto nº 8.789, de 29 de junho de 2016**. Dispõe sobre o compartilhamento de bases de dados na administração pública federal. Brasília: Presidência da República, [2016]. Disponível em: https://www.planalto.gov.br/ccivil_03/ato2015-2018/2016/decreto/d8789.htm . Acesso em: 13 mar. 2023.

¹¹⁹ CELLA; COPETTI, ref. 61, p. 42-43.

¹²⁰ “[...] a) os atributos biográficos; b) o número de inscrição no Cadastro de Pessoas Físicas - CPF; c) o número de inscrição no Cadastro Nacional de Pessoas Jurídicas - CNPJ; d) o Número de Identificação Social - NIS; e) o número de inscrição no Programa de Integração Social - PIS; f) o número de inscrição no Programa de Formação do Patrimônio do Servidor Público - Pasep; g) o número do Título de Eleitor; h) a razão social, o nome fantasia e a data de constituição da pessoa jurídica, o tipo societário, a composição societária atual e histórica e a Classificação Nacional de Atividades Econômicas - CNAE; e i) outros dados públicos relativos à pessoa jurídica ou à empresa individual;”. BRASIL, ref. 117.

¹²¹ BRASIL, ref. 117.

à existência de bem imóvel, localização do ato registral, números de inscrição e respectivas situações cadastrais no CPF e no CNPJ das partes envolvidas na operação;

II - informações constantes da declaração do Imposto sobre a Propriedade Territorial Rural relativas à existência de bem imóvel;

III - informações referentes a registros de natureza pública ou de conhecimento público constantes de nota fiscal;

IV - informações sobre parcelamento e moratória de natureza global dos débitos por ela administrados;

V - informações sobre débitos de pessoas jurídicas de direito público; e

VI - demais informações de natureza pública constantes das bases de dados sob sua gestão.

Art. 29. A Procuradoria-Geral da Fazenda Nacional disponibilizará aos órgãos interessados os seguintes dados não protegidos por sigilo fiscal:

I - dados constantes do termo de inscrição na dívida ativa da União e do Fundo de Garantia do Tempo de Serviço - FGTS;

II - informações sobre parcelamento e moratória de natureza global dos débitos inscritos em Dívida Ativa da União;

III - informações sobre débitos inscritos em dívida ativa da União, incluídos os de pessoas jurídicas de direito público e aqueles em fase de execução fiscal; e

IV - demais informações de natureza pública constantes das bases de dados sob a sua gestão.

O diploma ainda diferencia o compartilhamento de dados em diferentes níveis, a depender do grau de restrição de acesso das informações. Nessa senda, além do compartilhamento amplo de dados públicos, com vasta divulgação a todo e qualquer interessado, há o compartilhamento restrito – referente aos dados protegidos por sigilo, com concessão de acesso a todos os órgãos e a todas as entidades federais para a execução de políticas públicas – e o compartilhamento específico, também concernente aos dados protegidos por sigilo, com o fornecimento de acesso a órgãos e entidades específicos.

No compartilhamento restrito, o mecanismo e as regras devem ser estabelecidos pelo Comitê Central de Governança de Dados (CCGD), cujas competências estão dispostas nos arts. 21 e seguintes da norma. A esse órgão compete deliberar sobre diversos aspectos dessas operações, fixando orientações e diretrizes acerca da categorização dos diferentes tipos de compartilhamento, bem como sobre o desenho, os requisitos e as políticas de segurança em relação às bases de dados.

Ademais, para a hipótese do compartilhamento específico, as regras são definidas pelo gestor de dados, ou seja, o “órgão ou entidade responsável pela governança de determinado conjunto de dados” (art. 2º, inciso XIII)¹²².

Para a realização do compartilhamento de dados, a norma dispensa a

¹²² BRASIL, ref. 117.

celebração de qualquer convênio, acordo ou instrumento similar de cooperação entre os órgãos e entidades, mas, quando se tratar de dados pessoais em solicitações de interoperabilidade¹²³, o diploma prescreve a necessidade de explicitação quanto ao propósito legítimo, específico e explícito, à compatibilidade com a finalidade e ao compartilhamento do mínimo necessário para atendimento da finalidade (art. 5º, § 4º, incisos I a III).

Além disso, as plataformas de interoperabilidade devem “contemplar os requisitos de sigilo, confidencialidade, gestão, auditabilidade e segurança da informação necessários ao compartilhamento de dados, conforme regras estabelecidas pelo Comitê Central de Governança de Dados”, de modo que as ferramentas de gestão desses meios devem incluir mecanismos para que o gestor de dados possa ter conhecimento sobre o controle de acesso e o consumo dos dados (art. 7º, *caput* e parágrafo único).

Importante destacar, ainda, que a norma instituiu o Cadastro Base do Cidadão (CBC), cujos objetivos, entre outros, são os de “facilitar o compartilhamento de dados cadastrais do cidadão entre os órgãos da administração pública” e “realizar o cruzamento de informações das bases de dados cadastrais oficiais a partir do número de inscrição do cidadão no CPF” (art. 16, incisos V e VI)¹²⁴.

Segundo o art. 18, § 1º, os dados biográficos e cadastrais a serem inicialmente disponibilizados na base integradora são, no mínimo, os seguintes: número de registro, data da inscrição e da alteração e situação cadastral do Cadastro de Pessoas Físicas (CPF), nome completo, nome social, data de nascimento, sexo, filiação, nacionalidade, naturalidade e indicador e data de óbito.

No entanto, o § 2º desse mesmo artigo esclarece, sem definir qualquer parâmetro, que essa base será alimentada com outros dados pelo número de inscrição do CPF do cidadão.

Em novembro de 2022, com a edição do Decreto nº 11.266/2022¹²⁵, foi

¹²³ Segundo o decreto (art. 2º, inciso XVIII), interoperabilidade é a “capacidade de diversos sistemas e organizações trabalharem em conjunto, de modo a garantir que pessoas, organizações e sistemas computacionais troquem dados”. BRASIL, ref. 117.

¹²⁴ BRASIL, ref. 117.

¹²⁵ BRASIL. **Decreto nº 11.266, de 25 de novembro de 2022**. Altera o Decreto nº 10.046, de 9 de outubro de 2019, 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. Brasília: Presidência da República, [2022]. Disponível em: https://www.planalto.gov.br/ccivil_03/ato2019-2022/2022/Decreto/D11266.htm#art1. Acesso em: 13 mar. 2023.

acrescido o § 7º ao dispositivo, que determina a necessidade de “justificativa formal detalhada, em consonância com os princípios da proporcionalidade, da razoabilidade e da proteção de dados pessoais”, para a inclusão de novos dados pessoais na base integradora e para a escolha de novas bases temáticas.

Conforme será explorado no próximo capítulo, as disposições do referido decreto foram objeto de impugnação, por meio da ADI nº 6.649¹²⁶ e da Arguição de Descumprimento de Preceito Fundamental (ADPF) nº 695¹²⁷. Isso porque as regras de compartilhamento ali previstas poderiam estar desrespeitando princípios básicos da proteção de dados, eis que, na visão dos requerentes – Conselho Federal da Ordem dos Advogados do Brasil (CFOAB) e Partido Socialista Brasileiro (PSB) –, permitiriam a transmissão ampla e irrestrita de informações entre os órgãos públicos federais, “sem a devida indicação de protocolos de ação e independentemente da precisa identificação dos agentes públicos envolvidos no tratamento”¹²⁸.

Nessa toada, sustentava-se a inconstitucionalidade do decreto presidencial, tendo em vista que, com a criação do CBC e do CCGD, haveria uma institucionalização de base de dados unificada que poderia ser livremente compartilhada pelos órgãos públicos federais, o que violaria as diretrizes da LGPD e poderia acarretar riscos de vazamentos e de incidentes de segurança. Afirmava-se, ainda, que foram empregados conceitos vagos e genéricos para ampliar a base de dados dos cidadãos brasileiros, o que poderia potencializar a capacidade de controle político da população.

2.2.2 Decreto nº 10.209/2020

O governo federal também buscou disciplinar o compartilhamento de informações protegidas pelo sigilo fiscal na esfera da investigação e apuração de ilícitos administrativos. Por meio do Decreto nº 10.209, de 22 de janeiro de 2020¹²⁹,

¹²⁶ BRASIL. Supremo Tribunal Federal. **ADI nº 6.649**. Rel. Min. Gilmar Mendes. Brasília, DF, Plenário, j. 15/9/2022, DJ 19/6/2023. Disponível em: <https://jurisprudencia.stf.jus.br/pages/search/sjur482122/false>. Acesso em: 6 out. 2023.

¹²⁷ BRASIL. Supremo Tribunal Federal. **ADPF nº 695**. Rel. Min. Gilmar Mendes. Brasília, DF, Plenário, j. 15/9/2022, DJ 19/6/2023. Disponível em: <https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=768683763>. Acesso em: 6 out. 2023.

¹²⁸ BRASIL, ref. 126, p. 9.

¹²⁹ BRASIL. **Decreto nº 10.209, de 22 de janeiro de 2020**. Dispõe sobre a requisição de informações e documentos e sobre o compartilhamento de informações protegidas pelo sigilo fiscal. Brasília:

o Poder Executivo regulamentou a aplicação do aludido art. 198 do CTN, que veda “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”.

Dessa forma, estabeleceu a norma que os órgãos do Ministério da Fazenda deveriam fornecer à Controladoria-Geral da União (CGU), entidade federal responsável pela defesa da transparência na gestão e do patrimônio público, os dados necessários às atividades de supervisão da Administração Pública.

O decreto permite o compartilhamento de dados sob sigilo fiscal, mediante instrumento próprio, desde que haja solicitação direta, nos termos do inciso II do § 1º do art. 198 do CTN, “quando existir interesse da administração pública e comprovada a instauração regular de processo administrativo no órgão com o objetivo de investigar o sujeito passivo a que se refere a informação por prática de eventual infração administrativa”. Além disso, com base no § 2º do art. 198 do CTN, também é possibilitado o intercâmbio de informação sigilosa, desde que a operação seja “indispensável à realização de procedimentos de auditoria ou de inspeção de dados, de processos ou de controles operacionais da administração tributária e aduaneira, da gestão fiscal ou da análise de demonstrações financeiras da União”¹³⁰.

Para que possa haver a modalidade de intercâmbio de informações, deve-se instaurar previamente um processo administrativo em que haja clara definição do objetivo e do escopo da auditoria. Demais disso, também se exige a emissão de recibo referente à entrega dos dados, bem como uma manifestação fundamentada contendo esclarecimentos sobre a pertinência temática da informação com o objeto da atividade de inspeção e a necessidade e indispensabilidade de acesso, com a indicação de que o trabalho não poderia ser realizado ou que o seu resultado não poderia ser alcançado por outro meio.

Por fim, também se ressalta a imprescindibilidade da restrição do uso dos

Presidência da República, [2020]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/d10209.htm. Acesso em: 13 maio 2023.

¹³⁰ “[...] § 1º Excetua-se do disposto neste artigo, além dos casos previstos no art. 199, os seguintes: [...]”

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.” BRASIL, 1966.

dados ao fim específico de “realização de auditoria ou de inspeção de dados, de processos ou de controles operacionais da administração tributária e aduaneira, da gestão fiscal ou na análise de demonstrações financeiras da União” (art. 3º, § 1º, inciso IV).

São vedadas solicitações de acesso a dados genéricos, desproporcionais, imotivados ou desvinculados dos procedimentos de auditoria ou inspeção e a publicização de informações protegidas por sigilo fiscal ou profissional ou o repasse delas a terceiros.

A CGU tem o dever de manter as informações recebidas em sigilo, e o órgão receptor dos dados deve garantir, no mínimo, os mesmos requisitos de segurança da informação e de comunicações adotados pelo órgão cedente. Nesse particular, o órgão cedente e os seus servidores respondem exclusivamente por atos próprios e não podem ser responsabilizados por ação ou omissão que implique violação do sigilo pelo receptor.

O Tribunal de Contas da União (TCU) também poderá, no que couber, requisitar os dados por meio dos mecanismos previstos no decreto (art. 9º). Com tal previsão, o diploma inseriu a Corte de Contas no âmbito do processo de tratamento de dados fiscais, com vistas a aperfeiçoar os meios de monitoramento do órgão. Com isso, a regra atrai os órgãos tributários para dentro do processo de supervisão de contas públicas pelo TCU, que passa a contar com importantes ferramentas administrativas de vigilância das operações de fiscalização e de cobrança de tributos.

2.2.3 Portaria RFB nº 34/2021

Como decorrência do procedimento de governança estabelecido no Decreto nº 10.046/2019, foi editada a Portaria RFB nº 34, de 14 de maio de 2021¹³¹, que regulamenta o compartilhamento de dados não protegidos por sigilo fiscal, pela Receita Federal, com órgãos e entidades da Administração Pública federal direta, autárquica e fundacional e demais Poderes da União.

¹³¹ BRASIL. Secretaria Especial da Receita Federal do Brasil. **Portaria RFB nº 34, de 14 de maio de 2021**. Dispõe sobre o compartilhamento de dados não protegidos por sigilo fiscal com órgãos e entidades da Administração Pública Federal direta, autárquica e fundacional e dos demais Poderes da União. Diário Oficial da União, Brasília, DF, 18 maio 2021, seção 1, p. 64. Disponível em: <http://normas.receita.fazenda.gov.br/sijut2consulta/link.action?idAto=117598>. Acesso em: 18 maio 2023.

Segundo o art. 1º do referido ato normativo, podem ser disponibilizadas as seguintes informações constantes de bases de dados da RFB: Cadastro de Pessoas Físicas (CPF); Cadastro de Atividade Econômica da Pessoa Física (CAEPF); Cadastro Nacional da Pessoa Jurídica (CNPJ); Cadastro de Imóveis Rurais (Cafir); Cadastro Nacional de Obras (CNO); Cadastro do Simples Nacional; Declaração de Operações Imobiliárias (DOI); Nota Fiscal Eletrônica (NF-e); Sistemas de controle de débitos de pessoas jurídicas de direito público; Sistemas de controle de débitos parcelados; e Sistema de emissão de Certidão de Regularidade Fiscal perante a Fazenda Nacional.

Os órgãos e as entidades interessados em obter acesso a esses dados devem formalizar uma solicitação à RFB, na qual devem constar (i) a identificação do solicitante, bem como de seu dirigente e dos responsáveis pelos assuntos atinentes à contratação de serviços e à Tecnologia da Informação e Comunicação (TIC), (ii) a relação detalhada dos dados requeridos, (iii) a descrição da forma e da periodicidade de recebimento dos dados solicitados¹³², (iv) a demonstração da necessidade do compartilhamento e das finalidades de uso dos dados solicitados, (v) a indicação das bases de dados administradas pelo órgão ou entidade solicitante, de modo a possibilitar que a RFB verifique quais informações são de interesse da Administração Tributária federal, (vi) a declaração quanto ao cumprimento dos requisitos de segurança definidos pelo Comitê de Tecnologia e Segurança da Informação da Receita Federal (CTSI/RFB)¹³³ e (vii) a concordância com os termos e as disposições previstos na Portaria.

Merece destaque o art. 5º, que dispõe sobre a obrigação do órgão ou da entidade de utilizar corretamente as informações que receber ou tiver acesso. O § 1º desse dispositivo determina que os dados somente poderão ser utilizados nas

¹³² O fornecimento pode se dar de forma eventual ou continuada.

¹³³ O CTSI tem competência para deliberar sobre as diretrizes e investimentos em tecnologia e segurança da informação no âmbito da RFB. O órgão é composto pelos seguintes membros: Subsecretário-Geral da RFB; Subsecretário de Gestão Corporativa; Subsecretário de Arrecadação, Cadastros e Atendimento; Subsecretário de Administração Aduaneira; Subsecretário de Fiscalização; Subsecretário de Tributação e Contencioso; Coordenador-Geral de Tecnologia e Segurança da Informação; Coordenador-Geral de Planejamento, Organização e Avaliação Institucional; e Encarregado pelo Tratamento de Dados Pessoais da RFB. Cf. BRASIL. Secretaria Especial da Receita Federal do Brasil. **Portaria RFB nº 229, de 26 de fevereiro de 2013**. Institui o Comitê de Tecnologia e Segurança da Informação no âmbito da Secretaria da Receita Federal do Brasil e dá outras providências. Diário Oficial da União, Brasília, DF, 27 fev. 2013, seção 1, p. 91. Disponível em: <http://normas.receita.fazenda.gov.br/sijut2consulta/link.action?naoPublicado=&idAto=39727&visao=anotado>. Acesso em: 18 maio 2023.

atividades que, em virtude de lei, são de competência do órgão ou da entidade solicitante, que não poderá transferi-los a terceiros ou divulgá-los. Além disso, a utilização dos dados fornecidos em desconformidade com a legislação pertinente implica o imediato cancelamento do compartilhamento, sem prejuízo de apuração de eventual responsabilização (art. 5, § 2º).

A decisão sobre a viabilidade de atendimento ao pedido de disponibilização de dados compete ao Subsecretário-Geral da RFB (art. 9º). Se positiva, a norma prevê uma série de procedimentos a serem adotados pelo solicitante para que possa proceder com o processo de fornecimento (art. 9º, § 1º), quais sejam: mecanismos específicos para a disponibilização dos dados, acompanhamento pela Coordenação-Geral de Gestão de Cadastros e Benefícios Fiscais (Cocad) e obrigações, compromissos e responsabilidades previstas na portaria.

Como se nota, a Portaria RFB nº 34/2021 estipulou um vasto compartilhamento de informações armazenadas pelo Fisco federal. Importante observar que, embora o ato normativo preveja critérios relacionados à obrigatoriedade de se justificar as requisições, não há, em momento algum, a necessidade de se dar ciência ao titular dos dados.

Sobre esse aspecto, é importante ressaltar que a LGPD, em seu art. 5º, inciso XVI, prevê a possibilidade da operação de uso compartilhado, a qual é definida como a partilha de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais. O art. 18, inciso VII, por outro lado, dispõe sobre o direito do titular de dados de obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição, “informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados”¹³⁴.

Dessa maneira, é dever da autoridade ter o controle e informar quem são os destinatários de seus compartilhamentos. Isso impede que a Administração transforme suas bases em uma unidade informacional com o compartilhamento irrestrito de dados dos usuários dos serviços públicos.

Portanto, ainda que não haja expressa previsão, nada impede que sejam requisitadas informações acerca das operações previstas pela Portaria nº 34/2021, o que, contudo, pode ser impraticável, visto que o contribuinte não é noticiado sobre

¹³⁴ BRASIL, ref. 22.

esses compartilhamentos. Em outras palavras, isso demandaria que o cidadão tivesse conhecimento de um procedimento interno da Administração Pública que não lhe é informado, para, assim, poder pedir para ser comunicado.

2.2.4 Portaria RFB nº 81/2021

Ainda em 2021, a RFB também se preocupou em disponibilizar um serviço para que o titular pudesse compartilhar seus dados fiscais com outras entidades habilitadas e terceiros. Com isso, por meio da Portaria RFB nº 81, de 11 de novembro de 2021¹³⁵, foi aprovada a criação do sistema “Compartilha Receita Federal”.

A ideia da plataforma, segundo o art. 1º da portaria, é a de permitir que os titulares, pessoas naturais e jurídicas, “autorizem o compartilhamento de dados e informações de sua titularidade, que estejam em posse da Secretaria Especial da Receita Federal do Brasil (RFB), com terceiros indicados na respectiva autorização”.

Esse sistema é ofertado dentro da própria plataforma virtual da RFB – Portal do Centro Virtual de Atendimento (Portal e-CAC) – e exige, para sua utilização, um nível elevado de certificação de autenticação da identidade digital do usuário¹³⁶.

Trata-se de serviço facultativo e sem qualquer ônus para os titulares das informações a serem compartilhadas. Em verdade, o que buscou o Fisco federal, por meio desse ato normativo, foi criar um canal que facilitasse essa transmissão de informações fiscais e, ao mesmo tempo, mantivesse o cumprimento dos padrões de segurança do sigilo impostos pelo órgão tributário.

Nessa toada, a RFB tem o papel de “criar, mediante autorização do titular, um arquivo criptografado com os dados e as informações a serem compartilhados” e “ampliar, de forma gradativa, o conjunto de dados e informações dos titulares passíveis de compartilhamento por meio do sistema” (art. 4º, incisos I e II). O arquivo criptografado deve ser entregue por meio da interface específica a ser

¹³⁵ BRASIL. Secretaria Especial da Receita Federal do Brasil. **Portaria RFB nº 81, de 11 de novembro de 2021**. Aprova o sistema Compartilha Receita Federal e estabelece regras para o fornecimento, a terceiros, de dados e informações no interesse de seus titulares. Diário Oficial da União, Brasília, DF, 1º dez. 2021, seção 1-B, p. 1. Disponível em: <http://normas.receita.fazenda.gov.br/sijut2consulta/link.action?idAto=121890>. Acesso em: 18 jun. 2023.

¹³⁶ Nos termos do art. 1º, inciso II, requer-se a “autenticação com identidade digital Prata ou Ouro da Plataforma Gov.br, nos termos da Portaria SEDGGME nº 2.154, de 23 de fevereiro de 2021”. BRASIL, ref. 135.

disponibilizada pelo Serviço Federal de Processamento de Dados (Serpro), empresa pública vinculada ao Ministério da Fazenda, que será remunerada diretamente pelo terceiro indicado para o recebimento dos dados. Essa interface deve contar com um mecanismo para o fornecimento pontual e pode ter sistema para o fornecimento massivo. Além disso, a inclusão dos conjuntos de dados no sistema deve ser “efetuada mediante autorização específica da RFB” (art. 5º, § 3º).

Por fim, a portaria prevê a disponibilização, para auditoria, por meio da tecnologia *blockchain*, das “evidências relacionadas ao pedido, cancelamento ou expiração do prazo de validade do pedido de compartilhamento de dados e informações” (art. 6º). A regra visa fortalecer o controle da Administração Tributária sobre os dados compartilhados, bem como em relação à devida observância dos prazos e das autorizações estabelecidas na norma.

2.2.5 Portaria RFB nº 167/2022

Também é válido citar a Portaria RFB nº 167/2022¹³⁷, que autoriza o Serviço Federal de Processamento de Dados (Serpro) a disponibilizar a terceiros o acesso a dados armazenados pela RFB.

A norma diferencia os dados a serem fornecidos entre aqueles disponíveis no *site* da RFB, mediante transparência ativa – listados no Anexo I – e aqueles disponíveis em sistemas da Receita Federal, sob controle de acesso específico – previstos no Anexo II. No Anexo II, são descritos inúmeros dados sigilosos passíveis de transmissão. É possível solicitar, por exemplo, detalhes de mensagens da Caixa Postal do contribuinte no sistema eletrônico da RFB.

Por conta dessa sensibilidade, o art. 4º da norma dispõe que o tratamento de dados pessoais objeto da norma deve ocorrer para o fiel cumprimento de políticas públicas, em conformidade com o inciso III do *caput* do art. 7º da LGPD. No entanto, as regras previstas nessa portaria levantaram inúmeros questionamentos em relação à segurança das operações a serem procedidas pelo Serpro. Isso, inclusive, levou a RFB a publicar uma “Nota de Esclarecimento”, pela qual foram veiculadas

¹³⁷ BRASIL. Secretaria Especial da Receita Federal do Brasil. **Portaria RFB nº 167, de 14 de abril de 2022**. Autoriza o Serviço Federal de Processamento de Dados a disponibilizar acesso, para terceiros, dos dados e informações que especifica. Diário Oficial da União, Brasília, DF, 19 abr. 2022, seção 1, p. 51. Disponível em: <http://normas.receita.fazenda.gov.br/sijut2consulta/link.action?idAto=123666>. Acesso em: 18 maio 2023.

algumas explicações sobre o ato normativo.

Segundo o texto, seriam “absolutamente improcedentes e infundadas quaisquer afirmações de que a Receita Federal autorizou o Serviço Federal de Processamento de Dados (Serpro) a ‘vender’ dados pessoais de pessoas físicas ou jurídicas”. A Receita Federal justificou a implementação dos referidos procedimentos, a fim de buscar uma “solução tecnológica de alta performance” que fosse “capaz de suportar elevado volume de acessos, sem ampliar ou permitir acesso a dados que já não estivessem disponíveis”¹³⁸.

O órgão fiscal justificou o ressarcimento ao Serpro em razão de o acesso alternativo ser facultativo ao cidadão ou à empresa, destacando que ainda é possível proceder com a obtenção gratuita, nos *sites* e portais da RFB, de informações como os dados da Situação Cadastral no CPF. Quanto às informações que possuem alguma restrição, assevera que “continuam com a mesma restrição de acesso na solução tecnológica de alta performance, desenvolvida pelo Serpro”. Em conclusão, destacou que o ato normativo não ampliou ou permitiu acesso a dados que já não estivessem disponíveis, mas apenas permitiu que o Serpro “disponibilize um outro canal de acesso às informações, com o mesmo nível de controle de acesso, e seja ressarcido por seus custos relativos tão somente à plataforma tecnológica de alta performance”¹³⁹.

Ocorre que, embora sejam resguardados os níveis de controle de acesso a depender da informação solicitada, o ato normativo traz a previsão de uma nova modalidade de compartilhamento, pelo contrato unilateral entre o Serpro e o terceiro solicitante, de informações tributárias significativamente sensíveis e amplas. Isso, sem dúvidas, pode alargar a margem para as quebras na segurança. Aliás, a norma sequer prevê um procedimento específico, com a indicação de um encarregado ou dos agentes de tratamento¹⁴⁰.

As preocupações são válidas e se justificam pela própria previsão do art. 3º

¹³⁸ Disponível em: <https://www.gov.br/receitafederal/pt-br/assuntos/noticias/2022/abril/nota-de-esclarecimento>. Acesso em: 23 maio 2023.

¹³⁹ Disponível em: <https://www.gov.br/receitafederal/pt-br/assuntos/noticias/2022/abril/nota-de-esclarecimento>. Acesso em: 23 maio 2023.

¹⁴⁰ Nos termos da LGPD, o encarregado é a “pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD)” e os agentes de tratamento são o controlador e o operador. O controlador e o operador são pessoas naturais ou jurídicas, de direito público e privado, responsáveis, respectivamente, pelas decisões e pelo tratamento de dados pessoais. BRASIL, ref. 22.

da portaria, que assegura a implementação de “processo de identificação de risco institucional ou risco ao sigilo da pessoa física ou jurídica a que se referem os dados e informações”.

2.2.6 Convênio ICMS nº 134/2016

Ainda que não tratem especificamente de tributo federal, também merecem destaque as normas editadas pelo Conselho Nacional de Política Fazendária (CONFAZ) no âmbito do Convênio ICMS nº 134, de 9 de dezembro de 2016¹⁴¹, que disciplina o fornecimento de informações de contribuintes do Imposto sobre Circulação de Mercadorias e Serviços (ICMS).

Algumas das cláusulas desse convênio estabelecem obrigações acessórias no bojo da cobrança do ICMS, determinando que as instituições financeiras forneçam dados sobre transações de seus clientes aos Fiscos estaduais. Por exemplo, a cláusula terceira prevê que as instituições e os intermediadores financeiros e de pagamento, integrantes ou não do Sistema de Pagamentos Brasileiro (SPB), devem enviar aos Estados “todas as informações relativas às operações realizadas pelos beneficiários de pagamentos que utilizem os instrumentos de pagamento de que trata este convênio, conforme leiaute previsto em Ato COTEPE/ICMS”.

Os instrumentos de pagamento previstos na norma eram: “cartões de débito, crédito, de loja (*private label*), transferência de recursos, transações eletrônicas do Sistema de Pagamento Instantâneo [SPI], e demais instrumentos de pagamento eletrônico” (cláusula segunda). Com o advento do Convênio ICMS nº 166, de 23 de setembro de 2022¹⁴², foi acrescentado o § 5º-A à cláusula terceira, o qual também

¹⁴¹ BRASIL. Conselho Nacional de Política Fazendária. **Convênio ICMS nº 134, de 9 de dezembro de 2016**. Dispõe sobre o fornecimento de informações prestadas por instituições e intermediadores financeiros e de pagamento, integrantes ou não do Sistema de Pagamentos Brasileiro – SPB, relativas às transações com cartões de débito, crédito, de loja (*private label*), transferência de recursos, transações eletrônicas do Sistema de Pagamento Instantâneo e demais instrumentos de pagamento eletrônicos [...]. Brasília, DF, [2016]. Disponível em: https://www.confaz.fazenda.gov.br/legislacao/convenios/2016/CV134_16. Acesso em: 13 mar. 2023.

¹⁴² BRASIL. Conselho Nacional de Política Fazendária. **Convênio ICMS nº 166, de 23 de setembro de 2022**. Altera o Convênio ICMS nº 134/16, que dispõe sobre o fornecimento de informações prestadas por instituições e intermediadores financeiros e de pagamento, integrantes ou não do Sistema de Pagamentos Brasileiro – SPB, relativas às transações com cartões de débito, crédito, de loja (*private label*), transferência de recursos, transações eletrônicas do Sistema de Pagamento Instantâneo e demais instrumentos de pagamento eletrônicos [...]. Brasília, DF, [2022]. Disponível

estabelece a obrigação de envio das transações via PIX de forma retroativa, desde o início dos serviços deste meio de pagamento.

Ademais, segundo o § 4º dessa cláusula, os bancos devem enviar as referidas informações desde janeiro de 2022, conforme cronograma disposto na norma. A partir de setembro de 2023, seria observado o prazo estipulado no *caput*, isto é, até o último dia do mês subsequente à operação.

Segundo a cláusula quarta, a RFB e as secretarias estaduais, por meio de procedimento administrativo, podem solicitar, independentemente da territorialidade, em arquivo impresso ou eletrônico, as informações dispostas no convênio, além de “informações complementares dos beneficiários de pagamento, estabelecimentos e usuários de seus serviços”.

A cláusula sexta, por sua vez, prevê que a RFB e as unidades federadas devem estabelecer o novo formato e o leiaute para o fornecimento das informações das transações realizadas. Por fim, o parágrafo único dessa cláusula dispõe que as unidades federadas poderão compartilhar entre si as informações provenientes dos arquivos que serão disponibilizados.

O Ato COTEPE/ICMS nº 65/2018¹⁴³, com a redação dada pelos Atos COTEPE/ICMS nº 37/2022 e nº 81/2022, instituiu o Manual de Orientações de leiaute da Declaração de Informações de Meios de Pagamentos (DIMP)¹⁴⁴, o qual operacionalizou o procedimento de fornecimento de dados entre Entes Federativos.

Da leitura dos dispositivos acima mencionados, verifica-se que essas normas impõem às instituições financeiras obrigações acessórias de fornecimento de informações sobre transações que sequer têm relação com o fato gerador do ICMS. O Convênio CONFAZ e o Manual de Orientação da COTEPE estipulam regras

em: https://www.confaz.fazenda.gov.br/legislacao/convenios/2022/CV166_22. Acesso em: 13 mar. 2023.

¹⁴³ BRASIL. Conselho Nacional de Política Fazendária. **Ato COTEPE/ICMS nº 65, de 19 de dezembro de 2018**. Dispõe sobre as especificações técnicas para a geração de arquivos referentes às informações prestadas por instituições e intermediadores financeiros e de pagamento, integrantes ou não do Sistema de Pagamentos Brasileiro – SPB, relativas às transações com cartões de débito, crédito, de loja (*private label*), transferência de recursos, transações eletrônicas do Sistema de Pagamento Instantâneo e demais instrumentos de pagamento eletrônicos [...]. Brasília, DF, [2018]. Disponível em: <https://www.confaz.fazenda.gov.br/legislacao/atos/2018/ato-cotepe-icms-65-18>. Acesso em: 13 mar. 2023.

¹⁴⁴ Nos termos do art. 1º, § 1º, desse ato, a DIMP “corresponde ao conjunto de registros de forma padronizada contendo as informações exigidas nas cláusulas terceira e terceira-A do Convênio ICMS 134/16, de 9 de dezembro de 2016, e será gerada obedecendo o regime de competência das transações, em um arquivo único por unidade federada, de forma digital, com transmissão via TED-TEF”.

genéricas em relação à disponibilização de dados sobre as contas de pessoas físicas e jurídicas.

Com isso, operações que não se adequam à hipótese de incidência do ICMS e, de forma ainda mais grave, sem qualquer procedimento administrativo previamente instaurado, são compartilhadas.

Nesse sentido, exsurtem questionamentos acerca da incompatibilidade desses atos normativos com o entendimento firmado pelo STF no julgamento da ADI nº 2.859¹⁴⁵ quanto ao regramento sobre a transmissão dos dados fiscais sigilosos, pois não foram observadas as condicionantes então fixadas pela Corte¹⁴⁶. Conforme decidido naquela ação, aos Estados e aos Municípios não é permitida a automaticidade da transmissão de informações pelas instituições bancárias, à luz do disposto no art. 6º da Lei Complementar nº 105/2001, uma vez que a matéria deve ser previamente regulamentada, nesses entes, de forma análoga à previsão do diploma legal federal.

Isso se torna ainda mais evidente ao se examinar a Tabela de Código Finalidade do arquivo, no Manual de Orientações de leiaute da Declaração de Informações de Meios de Pagamento (DIMP). Além do código “Cumprimento de intimação específica para um CPF/CNPJ referente ao período da fiscalização ou processo administrativo” (código 3), há códigos como “[...] transações de pagamento e transferências de recursos via instituição de pagamento ou financeira e de intermediação de serviços e de negócios” (código 1).

Além disso, no tópico referente ao “resumo mensal das operações financeiras”, há a seguinte observação¹⁴⁷:

Em caso de dúvida quanto ao enquadramento da transação ou quanto ao remetente do recurso, a transação deverá ser enviada. Os arquivos com finalidade 3 podem conter informações de contas referenciadas nos itens 'h' e 'i' do rol exaustivo citado na descrição deste registro, sendo excluídas as transações entre mesma titularidade.

Da leitura desse trecho do Manual nota-se que, caso a instituição financeira não saiba o enquadramento da operação, ainda assim deve enviar a transação à Administração Tributária. Mesmo que não se tenha conhecimento se o crédito em

¹⁴⁵ BRASIL, ref. 87.

¹⁴⁶ Cf. o tópico sobre Sigilo Fiscal, no Capítulo I.

¹⁴⁷ Disponível em: <https://www.confaz.fazenda.gov.br/legislacao/arquivo-manuais/a13-anexo-ii-manual-de-orientacao-dimp-v09.pdf>. Acesso em: 10 maio 2023.

conta tem qualquer relação com operações tributadas pelo ICMS, e sem a comprovação da instauração prévia de procedimento fiscal ou da existência de processo administrativo em curso, impõe-se esse dever de compartilhamento.

Diante dessas considerações, o Convênio CONFAZ em questão levanta indagações sobre possíveis violações a preceitos constitucionais, bem assim à orientação dada pelo STF sobre o assunto. Inclusive, a norma foi impugnada por meio da ADI nº 7.276, ajuizada pela Confederação Nacional do Sistema Financeiro (CONSIF) e ainda será examinada pela Corte em sede de controle concentrado de constitucionalidade.

2.3 Mecanismos de proteção de dados

Como ensina Miriam Wimmer, o grande desafio para as legislações que tratam da proteção de dados é “encontrar um ponto de equilíbrio que leve em consideração a dupla natureza dos dados pessoais”. Segundo explica a autora, os dados são, ao mesmo tempo, a “projeção da personalidade humana, configurando-se estes como merecedores de ampla proteção pela ordem jurídica” e um “insumo essencial ao desenvolvimento das mais variadas atividades econômicas e governamentais, o que requer o estabelecimento de regras claras quanto às possibilidades de seu tratamento legítimo em variados contextos”¹⁴⁸.

Para as finalidades ora investigadas, a LGPD, Lei nº 13.709, de 14 de agosto de 2018, prevê uma série de definições específicas relevantes, que serão a seguir detalhadas.

Segundo o art. 5º da norma, *dado pessoal* é a “informação relacionada a pessoa natural identificada ou identificável” (inciso I), ao passo que *dado pessoal sensível* é o “dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural” (inciso II)¹⁴⁹.

Ademais, em seu art. 6º, a lei define os princípios que, juntamente com a boa-

¹⁴⁸ WIMMER, Miriam. Cidadania, tecnologia e governo digital: proteção de dados pessoais no Estado movido a dados. In: BARBOSA, Alexandre F. (Org.). **TIC Governo Eletrônico 2019**. Pesquisa sobre o uso das tecnologias de informação e comunicação no setor público brasileiro. 1. ed. São Paulo: Comitê Gestor da Internet no Brasil, 2020. p. 30.

¹⁴⁹ BRASIL, ref. 22.

fé, devem orientar o tratamento de dados. Dentre eles, destacam-se: (i) a finalidade, que estipula a “realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades”; (ii) a adequação, configurada pela “compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento”; (iii) a necessidade, definida como a “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) o livre acesso, que seria a “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) a transparência, isto é, a “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”¹⁵⁰; (vi) a segurança, a ser garantida pela “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”; (vii) a prevenção, a partir da “adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais”; e (viii) a responsabilização e prestação de contas, com a “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”¹⁵¹.

A LGPD dispõe, inclusive, no âmbito do direito ao livre acesso, sobre a garantia de obtenção facilitada, pelo titular, de informações sobre o tratamento de seus dados, que devem ser disponibilizadas de forma clara, adequada e ostensiva. Nesse ponto, os incisos do art. 9º preceituam a imposição de transparência quanto aos seguintes aspectos da operação: a finalidade específica, a forma e a duração, a identificação e o contato do controlador, as informações sobre o uso compartilhado,

¹⁵⁰ No âmbito do RGPD, observa-se o “princípio da viseira aberta” (*Grundsatz des offenen Visier*), segundo o qual o legislador europeu deve garantir que os titulares dos dados, no momento da coleta, sejam devidamente informados sobre os objetivos e os processos de tratamento posteriores. Trata-se de alusão ao direito que regula a atuação policial no tocante à coleta de dados para fins de investigação. Esse princípio impõe que o policial, ao abordar o investigado para coletar suas informações pessoais, seja por ele reconhecível. Sob o prisma da proteção de dados, significa dizer que o titular dos dados deve sempre poder reconhecer quem realiza a coleta de seus dados, bem como a finalidade da autoridade fiscalizadora. Cf. SEER, 2020.

¹⁵¹ BRASIL, ref. 22.

a responsabilidade dos agentes no tratamento e os direitos do titular.

O diploma legal também estabelece a possibilidade de disponibilização de “outras características previstas em regulamentação para o atendimento do princípio do livre acesso” (art. 9º, *caput*). O detalhamento dessa regra traria um importante avanço em matéria de proteção de dados, eis que conferiria maior segurança jurídica, com uma orientação mais precisa direcionada ao titular acerca da garantia de controle de suas informações¹⁵².

Em harmonia com o princípio do livre acesso, o art. 18 também assegura alguns direitos ao titular em face do controlador. Segundo esse dispositivo, o usuário, a qualquer momento e mediante requisição, pode exigir do controlador as seguintes medidas ou informações¹⁵³:

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

A exigência dessas medidas deve ser endereçada, mediante requerimento expresso, ao agente de tratamento (art. 18, § 3º). O titular também tem o direito de peticionar perante a Autoridade Nacional de Proteção de Dados (ANPD) para reivindicar suas garantias em relação aos seus dados pessoais (art. 18, § 1º).

No que atine especificamente ao processamento de dados por pessoas jurídicas de direito público, o art. 7º, inciso III, prevê a possibilidade de tratamento e compartilhamento para a consecução de políticas públicas previstas em lei e regulamentos, ou estabelecidas em contratos, convênios ou instrumentos congêneres. Demais disso, o art. 11, inciso II, alínea *b*, permite o tratamento de dados pessoais sensíveis, sem fornecimento de consentimento do titular, para o

¹⁵² Destaque-se que, nos termos da LGPD (art. 5º, inciso V), titular é a “pessoa natural a quem se referem os dados pessoais que são objeto de tratamento”. BRASIL, ref. 22.

¹⁵³ BRASIL, ref. 22.

“tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos”.

Em capítulo reservado às atribuições do Poder Público na matéria, é ressaltada a necessidade de o tratamento buscar atender à finalidade pública, na persecução do interesse coletivo, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público (art. 23).

Nessa perspectiva, é necessário que sejam comunicadas as situações em que, no exercício de suas competências, as autoridades realizam o tratamento de dados pessoais, sendo obrigatório o fornecimento de informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades. Essas informações devem estar dispostas em veículos de fácil acesso, preferencialmente na internet (art. 23, inciso I). Além disso, segundo o art. 23, inciso III, a Administração precisa indicar um encarregado, quando realizadas operações de tratamento de dados pessoais, nos termos do art. 39 da lei¹⁵⁴. Esse dispositivo “representa uma novidade no contexto brasileiro, com consequências ainda não plenamente avaliadas no âmbito do aparato estatal”¹⁵⁵.

Em complemento, o art. 26 orienta que esse uso compartilhado de dados pessoais pelas autoridades “deve atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios de proteção de dados pessoais elencados no art. 6º desta Lei”¹⁵⁶. Aqui, mais uma vez, o diploma legal deixou expressa a necessidade de se ter bem definida a finalidade do tratamento para toda e qualquer operação.

Por fim, também é relevante analisar o regramento sobre a transferência internacional de dados previsto na LGPD. A lei elenca as hipóteses em que essa operação é permitida¹⁵⁷:

Art. 33. [...]

I - para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto nesta Lei;

II - quando o controlador oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados

¹⁵⁴ “Art. 39. O operador deverá realizar o tratamento segundo as instruções fornecidas pelo controlador, que verificará a observância das próprias instruções e das normas sobre a matéria.” BRASIL, ref. 22.

¹⁵⁵ WIMMER, 2020, p. 32.

¹⁵⁶ BRASIL, ref. 22.

¹⁵⁷ BRASIL, ref. 22.

previstos nesta Lei, na forma de:

- a) cláusulas contratuais específicas para determinada transferência;
- b) cláusulas-padrão contratuais;
- c) normas corporativas globais;
- d) selos, certificados e códigos de conduta regularmente emitidos;
- III - quando a transferência for necessária para a cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução, de acordo com os instrumentos de direito internacional;
- IV - quando a transferência for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiro;
- V - quando a autoridade nacional autorizar a transferência;
- VI - quando a transferência resultar em compromisso assumido em acordo de cooperação internacional;
- VII - quando a transferência for necessária para a execução de política pública ou atribuição legal do serviço público, sendo dada publicidade nos termos do inciso I do caput do art. 23 desta Lei;
- VIII - quando o titular tiver fornecido o seu consentimento específico e em destaque para a transferência, com informação prévia sobre o caráter internacional da operação, distinguindo claramente esta de outras finalidades; ou
- IX - quando necessário para atender as hipóteses previstas nos incisos II, V e VI do art. 7º desta Lei.

Para o cumprimento do disposto no inciso I, o parágrafo único do art. 33 estabelece a possibilidade de órgãos públicos integrantes da administração direta dos Poderes Executivo, Legislativo e Judiciário e do Ministério Público, bem como autarquias, fundações públicas, empresas públicas, sociedades de economia mista e demais entidades controladas direta ou indiretamente pela União, Estados, Distrito Federal e Municípios (art. 1º, parágrafo único, da Lei de Acesso à Informação¹⁵⁸) requererem à autoridade nacional a “avaliação do nível de proteção a dados pessoais conferido por país ou organismo internacional”¹⁵⁹.

Para tal averiguação, a autoridade nacional deve considerar os critérios gerais listados no art. 34 da norma; quais sejam: a legislação vigente no país de destino ou no organismo internacional, a natureza dos dados, a observância dos princípios gerais de proteção de dados pessoais e os direitos previstos na própria LGPD, a adoção de medidas de segurança legalmente previstas, as garantias judiciais e institucionais existentes para que se possa garantir o respeito aos direitos de proteção de dados pessoais e outras circunstâncias específicas.

A norma traz diretrizes para que se possa ter informações precisas e

¹⁵⁸ BRASIL. **Lei nº 12.527, de 18 de novembro de 2011**. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Brasília: Presidência da República, [2011]. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2011/Lei/L12527.htm#art1. Acesso em: 5 mar. 2023.

¹⁵⁹ BRASIL, ref. 22.

padronizadas acerca do referido “nível de proteção a dados pessoais” em cada organismo internacional ou país. Trata-se de regra que visa dar, previamente às operações de troca de informações, mais segurança às autoridades brasileiras.

Cabe destacar, também, o inciso VII do art. 33, o qual possibilita a transferência internacional para a execução de política pública ou atribuição legal do serviço público, sendo imperiosa a publicidade nos termos do inciso I do art. 23, anteriormente mencionado.

As regras acima configuram relevantes avanços inseridos na matéria sobre proteção de dados pessoais. No entanto, sob a perspectiva tributária, verifica-se que a LGPD não traz previsões específicas voltadas às operações do Fisco ou mesmo para os mecanismos de fiscalização pelos Entes Federativos. Isso poderia, em última análise, levantar questionamentos acerca da compatibilidade da lei com assuntos tributários¹⁶⁰.

Uma questão que ampara essa visão é a imprecisão terminológica empregada na norma ao se referir às atribuições do Poder Público. Ao fazer menção ao tratamento de dados pessoais pela Administração Pública, a lei restringe tal competência à execução de políticas públicas (art. 7º, inciso III).

Contudo, em relação a esse aspecto particular, uma leitura abrangente de todo o complexo normativo permite verificar que o art. 23 impõe hipótese complementar para esse tratamento, ao acrescentar o objetivo de “executar as competências legais ou cumprir as atribuições legais do serviço público”. Dessa forma, pode-se concluir que o legislador pretendeu ir além da execução de políticas públicas ao definir o alcance da LGPD no setor público¹⁶¹.

Portanto, havendo tais hipóteses autorizativas, conclui-se que as relações jurídico-tributárias também estão dentro dos contornos fixados pela LGPD, isto é, estão abarcadas pelos comandos que disciplinam as operações com as pessoas jurídicas de direito público previstos na norma.

Um outro marco normativo que também rege a questão sobre o uso de dados pelo Poder Público é a Lei nº 12.527, de 18 de novembro de 2011, a Lei de Acesso à Informação (LAI). Em alguns aspectos, a LAI adota uma lógica distinta daquela que se observa na LGPD. Enquanto, na LGPD, verifica-se uma ideia de proteção de dados pessoais e uma busca pela transparência como “garantia, aos titulares, de

¹⁶⁰ LIOTTI, 2022, p. 155.

¹⁶¹ Cf. WIMMER, 2021, p. 280.

informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento” (art. 6º, inciso VI)¹⁶², a LAI pauta o propósito da transparência quanto ao “tratamento da informação”¹⁶³ a partir de uma concepção calcada na cultura de transparência no âmbito da Administração Pública¹⁶⁴.

Uma rápida comparação entre as duas normas permite constatar algumas diferenças terminológicas consideráveis. O exemplo mais marcante talvez seja o fato de que a LAI não utiliza a expressão “tratamento de dados pessoais”.

A necessidade de uma padronização redacional, muito além de qualquer preciosismo, poderia evitar possíveis divergências interpretativas em relação a conceitos correlatos. Não se ignora que os diplomas legais foram elaborados em momentos distintos da história, com objetivos distintos. Entretanto, incumbe ao legislador o dever de uniformizar os comandos legais sobre o tema, com o objetivo de afastar quaisquer possibilidades de interpretações equivocadas.

2.4 Aplicabilidade das normas de proteção de dados pessoais às trocas de informações tributárias

Do exame dos comandos acima verifica-se que algumas das definições ainda são superficiais e pouco precisas, notadamente quando pensadas para a utilização no direito tributário.

É claro que a aplicação da LGPD à esfera pública comporta seus desafios particulares. Como exemplifica Miriam Wimmer, seria ilógico presumir, invocando-se a proteção de dados pessoais, que o cidadão teria o direito de requerer a portabilidade de seus dados armazenados em determinado acervo governamental, ou que o indivíduo teria autonomia para consentir ou rejeitar o processamento de sua declaração de IR pela Receita Federal¹⁶⁵.

Direitos como de anonimização, de bloqueio ou de eliminação de dados desnecessários ou excessivos vão encontrar limitações quanto à sua aplicação no âmbito do Poder Público. Isso se dá em razão de eventual confronto com princípios gerais do direito administrativo, a exemplo da formalidade dos atos processuais,

¹⁶² BRASIL, ref. 22.

¹⁶³ BRASIL, ref. 158.

¹⁶⁴ Cf. WIMMER, 2021, p. 276.

¹⁶⁵ *Ibid.*, p. 278-279.

bem assim “em decorrência do conflito com normas concretas que disciplinam a forma e os prazos para guarda e arquivamento de registros e de documentos oficiais”¹⁶⁶.

Evidentemente, as relações com o Poder Público exigem contornos diferenciados. Afinal, diferentemente dos vínculos entre atores privados, o liame com o Poder Público tem caráter compulsório.

Por conta disso, inclusive, que a atividade estatal deve estar adstrita às competências específicas legalmente previstas. Nessa linha, também se faz necessário assegurar que os dados sejam utilizados apenas para os fins fiscais desejados. Afinal, para que se cumpra o princípio da necessidade, o processamento não pode exceder o “mínimo necessário” para alcançar os seus objetivos.

Nesse particular, um outro ponto crítico é a questão de a LGPD não estipular qualquer prazo específico para que a autoridade fiscal retenha os dados, o que também tem relação direta com a observância do princípio do mínimo necessário¹⁶⁷. Essa questão ganha especial relevância quando examinada em conjunto com os arts. 25 e 26 do diploma legal, que preveem expressamente a obrigação de os dados serem mantidos em formato interoperável e estruturado para o uso compartilhado. Tais disposições visam facilitar o processo de troca de informações entre os órgãos da Administração Pública, com o intuito específico de promoção de políticas públicas.

Por essas razões, em que pese a nítida intenção do legislador de assegurar a obediência ao princípio da eficiência administrativa, a falta de prazos bem definidos para a retenção de dados é um empecilho que se agrava em um cenário de interoperabilidade, isto é, de troca de informações entre diferentes bases de entidades do Poder Público.

Igualmente relevante é a questão da automação do processamento de dados, fenômeno inerente aos avanços tecnológicos que permeiam a atividade tributária na nova Era da Informação. Se, por um lado, o crescente protagonismo da tecnologia tem trazido diversas vantagens ao Sistema Tributário, ao permitir uma análise mais eficiente e automatizada do grande volume de dados – o que pode, inclusive, minimizar erros e economizar tempo –, por outro, esse fenômeno causa constantes incertezas em relação ao nível de automação que pode ser usado sem que direitos

¹⁶⁶ WIMMER, 2020, p. 32.

¹⁶⁷ LIOTTI, 2022, p. 153.

de privacidade sejam violados¹⁶⁸.

Essa automação permite um processamento mais célere, o que pode acabar ocorrendo em detrimento do controle da quantidade e do tipo de informação pessoal que está sendo utilizada pelo Fisco. Por consequência, o controle qualitativo desses dados pessoais também resta prejudicado.

No entanto, uma decisão final tomada unicamente pelo tratamento automatizado, que impacte a esfera jurídica do contribuinte, é expressamente vedada pelo RGPD. Segundo o art. 22 desse regulamento, “[o] titular dos dados tem o direito de não ficar sujeito a nenhuma decisão tomada exclusivamente com base no tratamento automatizado, incluindo a definição de perfis, que produza efeitos na sua esfera jurídica ou que o afete significativamente de forma similar”¹⁶⁹.

Dessa forma, é imprescindível que seja conferido ao contribuinte o direito de recorrer das decisões proferidas em processos automatizados de coleta e tratamento de dados. Afinal, as normas que preveem a execução dessas atividades precisam igualmente definir as salvaguardas adequadas¹⁷⁰.

O art. 20 da LGPD, nessa linha, garante, ao titular dos dados, o direito de “solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade”¹⁷¹. A medida tutela um direito que busca evitar efeitos negativos e anti-isonômicos, a exemplo do *profiling*¹⁷², prática que permite agrupar e identificar contribuintes com base no risco de inadimplência.

Ressalte-se, contudo, que essa previsão assegura, nesse cenário, apenas um nível mínimo de proteção, que, se não for implementado em conjunto com práticas efetivas de transparência, as quais visem garantir a comunicação com o contribuinte, não serão plenamente efetivas.

Em outras palavras, com as necessárias ressalvas para a atividade pública,

¹⁶⁸ SCARCELLA, Luisa. Tax compliance and privacy rights in profiling and automated decision making. **Internet Policy Review**, v. 8, n. 4, p. 2, 2019. Disponível em: <https://policyreview.info/articles/analysis/tax-compliance-and-privacy-rights-profiling-and-automated-decision-making>. Acesso em: 25 jun. 2023.

¹⁶⁹ UNIÃO EUROPEIA, ref. 20.

¹⁷⁰ SCARCELLA, ref. 168.

¹⁷¹ BRASIL, ref. 22.

¹⁷² Cf. SCHERMER, Bart. Risks of profiling and the limits of data protection law. *In*: CUSTERS, Bart; CALDERS, Toon; SCHERMER, Bart; ZARSKY, Tal (Orgs.). **Discrimination and privacy in the information society: data mining and profiling in large databases**. v. 3. Berlim: Springer, 2013. p. 137-152.

esses procedimentos não podem ser realizados à revelia do contribuinte, principal interessado na relação. Luís Eduardo Schoueri e Mateus Calicchio Barbosa comparam o eventual desejo do agente público de ocultar a atividade tributária a uma citação atribuída ao Ministro das Finanças do Rei Luís XIV, Jean-Baptiste Colbert. Segundo os autores, Colbert dizia que “a arte da tributação consiste em depenar o ganso de modo a obter a maior quantidade de penas com a menor quantidade possível de grasnido”¹⁷³. Se essa arte for totalmente silenciosa, os direitos do contribuinte acabam sendo solapados.

Outro ponto que merece destaque é o fato de a LGPD apenas prever que o prazo para o controlador comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança apto a acarretar risco ou dano relevante aos titulares deve ser razoável, conforme definido pela autoridade nacional (art. 48, § 1º), sem determinar os critérios para essa situação de risco¹⁷⁴. Novamente, essa imprecisão quanto ao prazo pode afetar as garantias individuais¹⁷⁵.

Ademais, também é relevante observar que a ideia de se compartilhar apenas o que for imprescindível à operação, com base na leitura do princípio da necessidade, pode confrontar as trocas de informações que se dariam, por exemplo, pela AEol, já que essas ocorrem de maneira automatizada. Dessa forma, à luz das regras da LGPD, verifica-se um aparente conflito entre os interesses das autoridades fiscais e os direitos fundamentais dos contribuintes. O enfrentamento dessas imprecisões é de fundamental relevância para a aplicação das regras de proteção de dados pessoais às atividades fiscais.

Finalmente, um outro importante debate diz respeito à aplicabilidade dos comandos internacionais sobre a proteção de dados de contribuintes no direito interno. É bem verdade que o CTN estabelece, em seu art. 98, a revogação ou modificação da legislação tributária interna pelos tratados e pelas convenções internacionais. O dispositivo determina, ainda, a observância pelas leis supervenientes.

Dessa maneira, o art. 98 transmite a ideia de superioridade hierárquica dos tratados em relação à legislação interna. Contudo, vale lembrar que o STF, no julgamento da Medida Cautelar na Ação Direta de Inconstitucionalidade (ADI) nº

¹⁷³ SCHOUERI, Luís Eduardo; BARBOSA, Mateus Calicchio. Transparency: from tax secrecy to the simplicity and reliability of the tax system. **British Tax Review**, vol. 5, p. 666-681, 2013, p. 678-679.

¹⁷⁴ BRASIL, ref. 22.

¹⁷⁵ LIOTTI, 2022, p. 153.

1.480/DF, decidiu que “[o]s tratados ou convenções internacionais, uma vez regularmente incorporados ao direito interno, situam-se, no sistema jurídico brasileiro, nos mesmos planos de validade, de eficácia e de autoridade em que se posicionam as leis ordinárias”, o que ocasionaria, por consequência, entre as leis internas e os atos de direito internacional público, mera relação de paridade normativa.

Assim, concluiu a Corte que a eventual preponderância dos tratados ou convenções internacionais sobre as regras infraconstitucionais de direito interno somente se justifica quando “a situação de antinomia com o ordenamento doméstico impuser, para a solução do conflito, a aplicação alternativa do critério cronológico (*‘lex posterior derogat priori’*) ou, quando cabível, do critério da especialidade”¹⁷⁶.

Ocorre que, para temas tributários, houve interpretação diversa, como bem rememora o professor Hugo de Brito Machado Segundo¹⁷⁷:

Posteriormente, com o julgamento do RE [Recurso Extraordinário] 229.096, no qual o STF consignou que tratados internacionais podem, sim, servir de instrumento para a concessão de isenções de tributos estaduais e municipais [...], tornou-se inviável para a Corte Suprema manter o entendimento de que, apesar do art. 98 do CTN, os tratados internacionais, em matéria tributária, teriam *status* igual ao de uma lei ordinária federal. Isso chegou, inclusive, a ser mencionado no julgado, quando se destacou que o precedente em sentido contrário, bastante antigo, havia sido proferido por maioria de votos e em matéria de direito comercial (e não tributário, ao qual seria aplicável o art. 98 do CTN) [...]

No mencionado RE nº 229.096/RS, o STF assentou que o referido dispositivo, ao definir essa supremacia dos acordos internacionais, “outra coisa não fez senão explicitar a realidade jurídica, seja, o caráter geral e, pois, nacional dos tratados em matéria tributária”¹⁷⁸.

Assim, para acordos que versem sobre temas do direito tributário, é claro o entendimento de que deve prevalecer a norma internacional sobre a legislação tributária interna. Todavia, a LGPD não está abarcada pela regra, pois não é uma

¹⁷⁶ BRASIL. Supremo Tribunal Federal. **ADI nº 1.480 MC**. Rel. Min. Celso de Mello. Brasília, DF, Plenário, j. 04/09/1997, DJ 18/05/2001. Disponível em: <https://jurisprudencia.stf.jus.br/pages/search/sjur18417/false>. Acesso em: 8 out. 2023.

¹⁷⁷ SEGUNDO, Hugo de Brito Machado. **Código Tributário Nacional**: anotações à Constituição, ao Código Tributário Nacional e às Leis Complementares 87/1996 e 116/2003. 6. ed., São Paulo: Atlas, 2017. p. 223.

¹⁷⁸ BRASIL. Supremo Tribunal Federal. **RE nº 229.096/RS**. Rel. Min. Cármen Lúcia. Brasília, DF, Plenário, j. 16/8/2007, DJ 11/4/2008. Disponível em: <https://jurisprudencia.stf.jus.br/pages/search/sjur88728/false>. Acesso em: 8 out. 2023.

norma tributária. Na verdade, conforme já ressaltado, sequer dispõe – ainda que lateralmente – sobre essa temática.

Portanto, para os assuntos que circundam a LGPD, deve-se observar o entendimento firmado na ADI nº 1.480/DF, isto é, o da resolução pelos critérios da cronologia e da especialidade. Nessa senda, é certo que, por disciplinar normas gerais para toda a Administração Pública e, como demonstrado anteriormente, versar sobre o uso de dados em todos os serviços públicos, e não só para políticas públicas, a LGPD regulamenta também as operações fiscais.

Dessa forma, é necessário sempre garantir os critérios mínimos de proteção nesse universo. Na experiência comparada, desde a decisão sobre a Lei do Censo de 1983¹⁷⁹, o BVerfG consolidou sua jurisprudência em torno da ideia de se fixar os requisitos mínimos para que seja observada a proteção de dados no bojo da intervenção tributária.

Deve-se, nesse sentido, assegurar ao contribuinte, titular dos dados, certeza e clareza quanto à norma, explicitando-se o motivo, a finalidade e os limites da restrição do direito à privacidade¹⁸⁰.

Isso visa garantir maior segurança contra o uso indiscriminado de informações fiscais, isto é, os dados não devem ser direcionados para outras utilidades ou para o cruzamento com outros dados. Assim, é dever do legislador estabelecer a finalidade da coleta e determinar minimamente a autoridade destinatária nas operações de intervenção tributária. Essa regra se alinha ao princípio da necessidade previsto na Lei Geral.

Também não se pode perder de vista, como mencionado no tópico anterior, que, em linha com o direito ao livre acesso, a LGPD dispôs sobre o dever de informação da Administração Pública, bem assim sobre o direito de obtenção facilitada, pelo titular, de informações sobre o tratamento de seus dados (arts. 9º e 23).

Assim, ressalta-se, mais uma vez, a importância de uma regulamentação para o atendimento do princípio do livre acesso na seara tributária, a fim de se ter uma melhor definição sobre a aplicação das normas de proteção de dados nesse campo.

¹⁷⁹ Disponível em: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/1983/12/rs19831215_1_bvr020983en.html;jsessionid=27BB1B55B8E909DFDD46DB2D2AD88A2E.internet012. Acesso em: 25 maio 2023.

¹⁸⁰ SEER, 2020, p. 24-25.

Inclusive, o referido art. 18 escancara essa preocupação, pois prevê situações que não poderiam ser seguidas à risca nas relações jurídico-tributárias, mas que, em tese, são de observância obrigatória pelo Fisco, na condição de controlador.

Tendo essas controvérsias em mente, o próximo capítulo é destinado a investigar e propor, com base nos precedentes internos e externos, bem assim nas orientações internacionais, as devidas demarcações para as operações tributárias no cenário ora examinado.

CAPÍTULO III

OS STANDARDS PARA A ATUAÇÃO DO FISCO BRASILEIRO NA TRIBUTAÇÃO MOVIDA A DADOS

“As cláusulas que garantem ao indivíduo proteção contra abusos específicos de poder devem ter a mesma capacidade de adaptação a um mundo em transformação.”

(L. Brandeis)¹⁸¹

3.1 Considerações preliminares

As novas tecnologias e inovações, com o “caráter místico”¹⁸² a elas intrínseco, ainda carregam certo grau de incerteza no campo do estudo acerca dos seus limites, especialmente quando se fala em regras constitucionais contrapostas.

Tal qual restou decidido no Tema 225 da sistemática da repercussão geral¹⁸³ e na ADI nº 2.859¹⁸⁴, para que se possa conceber a mitigação dos direitos à privacidade e ao sigilo de dados, é necessário que haja, antes, uma fundamentação adequada, “por meio da qual sejam exteriorizadas as razões que permitem a superação da regra, inclusive para viabilizar o controle de tais razões, o que é fundamental para decidir quais casos podem ser decididos de forma semelhante”¹⁸⁵.

São essas razões, portanto, que devem guiar e definir as atribuições fiscalizatórias do Fisco. Nesse sentido, a amplitude das competências investigatórias conferidas à Administração Tributária é um elemento essencial para a fixação dos devidos parâmetros de atuação. Afinal, como aponta Jules Michelet Queiroz e Silva, no direito tributário, o amplo poder probatório dado ao órgão fiscalizador “justifica um

¹⁸¹ No original: “*Clauses guaranteeing to the individual protection against specific abuses of power must have a similar capacity of adaptation to a changing world*”. ESTADOS UNIDOS. Supreme Court of the United States. **Olmstead v. United States, 277 U.S. 438 (1928)**. Washington, 1928.

¹⁸² AFONSO, José Roberto; ARDEO, Thaís; MOTTA, Bernardo. Impactos da Revolução Digital na Tributação: uma primeira revisão bibliográfica. In: AFONSO, José Roberto; SANTANA, Hadassah Laís (Orgs.). **Tributação 4.0**. São Paulo: Almedina, 2020. p. 217-226.

¹⁸³ BRASIL, ref. 82.

¹⁸⁴ BRASIL, ref. 87.

¹⁸⁵ MARQUES; LIOTTI, 2021, p. 199.

standard protetivo em favor do contribuinte”, haja vista que, nessa matéria, há a “figura do dever de colaboração do contribuinte em prol do Fisco”¹⁸⁶.

O autor pontua que há uma espécie de dever probatório do contribuinte em favor dos interesses da Administração no bojo da sua fiscalização. Cita, a partir de uma perspectiva voltada para o direito brasileiro, as lições de Alberto Xavier, que define esse dever de cooperação como uma “obrigação do contribuinte de facultar ou apresentar os meios de provas necessários à instrução do procedimento administrativo e que serão valorados pela Administração Tributária”¹⁸⁷.

Por conseguinte, Jules Michelet sintetiza o tópico¹⁸⁸:

A Administração Tributária, portanto, pode fixar obrigações a serem cumpridas pelo contribuinte para aumentar a eficácia da fiscalização, seja pela via da contabilidade tributária cotidiana, seja por declarações específicas. Esse poder de estipular obrigações evidentemente confere um poder probatório ao Fisco, que decide quais documentos serão produzidos pelo contribuinte e, futuramente, poderão ser usados para instruir procedimentos de lançamento. O Fisco, com efeito, tem um poder probatório preventivo, estipulando a prova documental a ser produzida pelo contribuinte no interesse direto da apuração fiscal.

De fato, ante esse constante alargamento dos poderes inerentes ao dever de cooperação, não se pode perder de vista que “as informações coletadas ativa e passivamente pelo Fisco podem ser armazenadas em amplos bancos de dados que servirão à atividade arrecadatória, o que evidencia o poder informacional de fato exercido pela Administração”¹⁸⁹. Em meio a essa infinidade de informações que reside o problema desta pesquisa, haja vista a evidente possibilidade de se afetar o contribuinte, que se vê obrigado a fornecer os seus dados.

Em outras palavras, como pontua Miriam Wimmer, o debate é sobre o quão bem o Estado deve conhecer seus cidadãos. Com isso, surgem dois diferentes vetores interpretativos: de um lado, há o tratamento de dados pela Administração como pré-requisito para o exercício da cidadania e, do outro, os riscos de violações de direitos, decorrentes do aumento da quantidade e da variedade de informações

¹⁸⁶ Cf. QUEIROZ E SILVA, Jules Michelet Pereira. **Standards de Prova no Direito Tributário**. São Paulo: IBDT, 2022. p. 164-165.

¹⁸⁷ XAVIER, Alberto. Do lançamento: teoria geral do ato, do procedimento e do processo tributário. 2. ed. Rio de Janeiro: Forense, 1998, p. 149-151 *apud* QUEIROZ E SILVA, Jules Michelet Pereira. **Standards de Prova no Direito Tributário**. São Paulo: IBDT, 2022. p. 165.

¹⁸⁸ QUEIROZ E SILVA, 2022, p. 168.

¹⁸⁹ *Ibid.*, p. 169.

sob o domínio do Poder Público¹⁹⁰.

Nessa relação, o contribuinte coloca-se na posição de fornecedor de subsídios para que possa haver a devida investigação de eventuais fatos geradores, que dariam ensejo à tributação. Por sua vez, a autoridade fiscal, que não conseguiria tributar sem o fornecimento desses dados, recebe e processa essas informações.

Se não há dúvida do dever de colaboração dos contribuintes nessa relação, por outro lado, não se tem muita certeza sobre o papel das autoridades. Como advertem Luís Eduardo Schoueri e Mateus Calicchio Barbosa, o atual debate atinente à transparência fiscal parece estar orientado para um único sentido: só se exige do contribuinte esse dever sem que sejam cobradas contraprestações efetivas de *accountability* do Poder Público¹⁹¹.

Dessa forma, concluem os autores que essa abordagem unilateral deve ser repensada para que possa haver um “relacionamento maduro entre o Estado e o cidadão”, o que, segundo afirmam, “parece ser uma abordagem melhor para garantir que os contribuintes se sintam parte da comunidade e, portanto, envolvidos no processo de garantia, aos Estados, dos meios para a consecução de suas atividades” (tradução nossa)¹⁹².

No Brasil, a imposição de colaboração encontra guarida no art. 113, § 2º, do Código Tributário Nacional, que delega à legislação tributária a disciplina da obrigação acessória, isto é, confere a competência de a Administração Tributária estipular as regras voltadas para o supervisionamento das obrigações principais (art. 113, § 1º). Essa obrigação, segundo a norma, tem por objeto “as prestações, positivas ou negativas, nela previstas no interesse da arrecadação ou da fiscalização dos tributos”¹⁹³.

Nesse prisma, este capítulo apresenta os parâmetros para a atuação do órgão fazendário brasileiro tanto na sistemática de coleta, como na de repasse de

¹⁹⁰ WIMMER, 2021, p. 273.

¹⁹¹ SCHOUERI, Luís Eduardo; BARBOSA, Mateus Calicchio. Transparency: from tax secrecy to the simplicity and reliability of the tax system. **British Tax Review**, v. 5, p. 666-681, 2013. p. 678.

¹⁹² No original: “*These references seem to be enough reason to suggest that the unilateral approach to transparency should be reviewed, and that the holistic treatment of the theme should be included in the Action Plan, if one really believes in transparency as a mechanism for the creation of a mature relationship between state and citizen, which seems to be a better approach to making sure that taxpayers feel part of the community and therefore involved on the process of granting states the means for their activities*”. SCHOUERI, BARBOSA, 2013, p. 678.

¹⁹³ BRASIL, 1966.

informações dos contribuintes. Com isso, neste ponto da pesquisa, pretende-se definir quantos e quais dados a Administração Tributária pode processar e quais limites ela deve observar.

À vista disso, também são levantadas as hipóteses de responsabilização dos agentes públicos nas situações infracionais. Afinal, seguindo o dever de sigilo e de respeito à privacidade dos administrados, o compromisso recai não só sobre o Estado, mas também sobre os servidores responsáveis pelo tratamento. Nesse sentido, caso reste comprovada uma situação de negligência ou de dolo, o agente pode acabar respondendo em diferentes esferas pelo ato.

Por fim, sem a pretensão de esgotar o debate sob a perspectiva comparada, discorre-se sobre o panorama normativo internacional, a partir das diretrizes da OCDE, bem assim sobre relevantes precedentes no cenário global.

3.2 Coleta de dados

Um reflexo da intensificação da coleta de dados, no cenário brasileiro, pode ser notado a partir da constante digitalização de obrigações acessórias, a exemplo da declaração do IR. Hoje, os dados podem ser inseridos em uma plataforma *on-line* da Receita Federal, via internet¹⁹⁴, o que pode mudar a relação entre contribuintes e o Fisco ou o Judiciário.

Talvez por não ser obrigatório para todas as operações, o formato digital, com a utilização de certificado digital com base na Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), ainda não tenha sido maciçamente adotado pelas empresas, mas, com a virtualização das relações com as autoridades nacionais¹⁹⁵, espera-se que seu uso passe a ser obrigatório para diversas finalidades¹⁹⁶.

Contudo, como a operação de coleta de dados pressupõe o armazenamento

¹⁹⁴ Disponível em: <https://www.gov.br/receitafederal/pt-br/assuntos/meu-imposto-de-renda>. Acesso em: 27 fev. 2023.

¹⁹⁵ Muito por conta do uso do sistema “gov.br”, regulamentado pela Lei nº 14.129, de 29 de março de 2021. BRASIL. **Lei nº 14.129, de 29 de março de 2021**. Dispõe sobre princípios, regras e instrumentos para o Governo Digital e para o aumento da eficiência pública e altera a Lei nº 7.116, de 29 de agosto de 1983, a Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), a Lei nº 12.682, de 9 de julho de 2012, e a Lei nº 13.460, de 26 de junho de 2017. Brasília: Presidência da República, [2021]. Disponível em: https://www.planalto.gov.br/ccivil_03/ato2019-2022/2021/Lei/L14129.htm. Acesso em: 27 fev. 2023.

¹⁹⁶ Cf. PINHEIRO, Patricia Peck. **Direito Digital**. 7. ed. São Paulo: Saraiva Educação, 2021. p. 349-351.

de informações, é necessário que sejam bem desenhados os contornos para essa estocagem. Um ponto essencial desse debate é a importância de se ter bem definido, de acordo com a finalidade almejada pela autoridade tributária, o prazo para justificar a consecução da atividade, à luz da ideia de efetivação da pretensão tributária. Afinal, as atividades da Administração Tributária devem guardar, a todo momento, algum respaldo em sua atividade-fim; qual seja: a intenção de tributar.

Nesse sentido, rememore-se que o art. 17, par. 1, do RGPD dispõe sobre o direito ao apagamento de dados pessoais em alguns casos. Para o direito tributário, merece destaque a alínea *a*, que trata dos dados pessoais que não são mais necessários para a finalidade para a qual foram colhidos e tratados.

Um exemplo corriqueiro de um tratamento que perde supervenientemente seu objeto é o caso em que ocorre a prescrição da ação de cobrança do crédito tributário (CTN, art. 174). Nesse caso, não há mais a pretensão tributária, uma vez que o decurso do prazo prescricional gera a extinção do crédito (CTN, art. 156, inciso V)¹⁹⁷. Dessa forma, como ensina Roman Seer, “[s]e a pretensão tributária não mais existe, falta uma justificativa para se continuar mantendo os dados”¹⁹⁸. Se o armazenamento não for mais concomitante com a finalidade de se tributar para aquela atividade específica fiscalizada, a guarda de dados não encontra mais respaldo legal ou constitucional.

Além da necessidade de haver uma pretensão tributária, a atividade fiscalizadora deve valer-se de meios razoáveis para alcançar as suas finalidades arrecadatórias. Afinal, a simples existência de uma finalidade, por si só, não garante que se possa realizar toda e qualquer coleta. A seguir será abordado um julgamento paradigmático, em que o STF fixou alguns limites ao recolhimento de dados pessoais pelo Poder Público.

3.2.1 Juízo de adequação e necessidade: julgamento da ADI nº 6.387

No julgamento do referendo de medida cautelar concedida nas ADIs nº 6387, nº 6388, nº 6389, nº 6390 e nº 6393¹⁹⁹, o STF assentou algumas divisas para a

¹⁹⁷ Cf. AMARO, Luciano. **Direito Tributário Brasileiro**. 22 ed. São Paulo: Saraiva, 2017. p. 426-447.

¹⁹⁸ SEER, 2020, p. 39.

¹⁹⁹ BRASIL. Supremo Tribunal Federal. **ADI nº 6.387 MC-Ref**, Rel. Min. Rosa Weber. Brasília, DF, Plenário, j. 7/5/2020, DJ 12/11/2020. Disponível em: <https://jurisprudencia.stf.jus.br/pages/search/sjur436273/false>. Acesso em: 8 out. 2023.

coleta de dados pessoais dos cidadãos.

Discutia-se, nessas ações diretas, a constitucionalidade da Medida Provisória (MP) nº 954/2020, que, no contexto da pandemia, obrigava as operadoras de telefonia a fornecerem dados de seus usuários, como nomes, telefones e endereços, ao Instituto Brasileiro de Geografia e Estatística (IBGE). Pretendia-se, com o dispositivo, “realizar entrevistas em caráter não presencial no âmbito de pesquisas domiciliares” (art. 2º, § 1º)²⁰⁰.

As entidades autoras argumentavam que a finalidade da norma seria genérica e imprecisa, o que colocaria em risco a segurança dos dados dos indivíduos. Aduzia-se, assim, que a medida seria desproporcional e acabaria por invadir o campo da privacidade dos usuários de serviços de telefonia.

Prevaleceu, na Corte, o entendimento de que o diploma veiculava mecanismos de recolhimento de dados que afrontavam direitos fundamentais. Conforme se depreende das manifestações apresentadas, concluiu-se que, em face da permanente abertura da ordem constitucional às inovações tecnológicas, haveria a necessidade de que a interpretação da Constituição acompanhasse a evolução do conceito de privacidade. Além disso, apesar de o julgamento ser anterior à edição da Emenda Constitucional (EC) nº 115/2022, ali já se reconhecia a proteção de dados pessoais como um direito fundamental autônomo.

O Tribunal considerou que a autodeterminação só poderia ser afastada por uma justificação minudente e exaustiva das finalidades da coleta de informações. Esse dever instrumental não era observado na norma em apreço, que veiculava apenas o objetivo de “produção estatística oficial” para fundamentar o uso dos dados.

Essa simplicidade e vagueza da Medida Provisória também deixava de assegurar os requisitos básicos de transparência, que pudessem garantir ao cidadão um nível mínimo de controle sobre os dados extraídos. Nesse particular, ponderou-se que a Administração Pública possui o dever de conferir ao titular condições suficientes para monitorar a forma pela qual seus dados são utilizados. Isso,

²⁰⁰ BRASIL. **Medida Provisória nº 954, de 2020**. Dispõe sobre o compartilhamento de dados por empresas de telecomunicações prestadoras de Serviço Telefônico Fixo Comutado e de Serviço Móvel Pessoal com a Fundação Instituto Brasileiro de Geografia e Estatística, para fins de suporte à produção estatística oficial durante a situação de emergência de saúde pública de importância internacional decorrente do coronavírus (covid-19), de que trata a Lei nº 13.979, de 6 de fevereiro de 2020. Brasília: Presidência da República, [2020]. Disponível em: <https://www.congressonacional.leg.br/materias/medidas-provisorias/-/mpv/141619>. Acesso em: 10 maio 2023.

inclusive, é essencial para que se possa verificar, posteriormente, eventuais ilicitudes incorridas nessas operações.

O Ministro Gilmar Mendes destacou, em seu voto, que o legislador “não se desincumbiu do ônus de instituir salvaguardas técnicas e administrativas efetivas que pudessem colmatar a necessária proteção ao tratamento de dados”. Isso porque não foram estabelecidas, no texto legal, as formas de anonimização dos dados compartilhados, nem foram contemplados mecanismos minimamente eficientes de transparência no tratamento. Na verdade, a norma apenas atribuiu ao Presidente do IBGE o poder de estabelecer o “procedimento para a disponibilização dos dados” (art. 2º, § 2º)²⁰¹.

Com essas considerações, a Suprema Corte brasileira referendou a medida liminar que suspendia a eficácia da MP nº 954/2020 e, dessa forma, definiu relevantes balizas para a disciplina de proteção de dados pessoais, notadamente a definição da necessidade de imposição de mecanismos que assegurem a transparência em relação aos dados tratados.

Trata-se, nesse sentido, de regra crucial para que se possa assegurar o controle, pelo titular, do uso de suas informações pessoais. Essa orientação deve ser transplantada para o direito tributário, que, não raras as vezes, conta com atos normativos que instituem procedimentos de coleta e de armazenamento incompatíveis com a disciplina da privacidade, não prevendo a garantia mínima de comunicação com o contribuinte detentor dos dados.

3.3 Transferência de dados

O texto constitucional assegura não apenas a garantia individual ao sigilo de dados, mas, também, o resguardo do procedimento de transmissão²⁰². Dessa forma, muito além do intuito de se manter hígida a confidencialidade nessas operações, esse comando também visa assegurar a proteção do usuário de serviços públicos sob a perspectiva da necessidade e da proporcionalidade²⁰³.

Nesse sentido, muito embora as operações de transmissão de dados pessoais visem alcançar os objetivos cogentes do Poder Público, é imprescindível, à

²⁰¹ BRASIL, ref. 199.

²⁰² Inviolabilidade do sigilo das comunicações de dados (art. 5º, inciso XII, da Constituição Federal).

²⁰³ Cf. BLACK; STEVENS, 2013.

luz da Constituição Federal, que haja um diálogo com a salvaguarda do sigilo das comunicações de dados em sua concepção mais ampla. Por esse ângulo, a tutela da supremacia do interesse público, calcada na ideia de eficiência administrativa, precisa afastar qualquer visão dicotômica que a coloque em confronto com a manutenção da privacidade e da proteção de dados pessoais.

Ocorre que a visão da eficiência administrativa e da prevalência do interesse público remete a ideias como interesse geral e bem comum, “conceitos jurídicos dotados de elevado grau de indeterminação”, o que pode confrontar direitos e princípios que tutelam garantias individuais²⁰⁴.

Além disso, apesar da menção expressa aos princípios da finalidade e da adequação na transferência de dados, a LGPD não especifica as consequências para a hipótese de utilização desviante pelo Poder Público. A lei preceitua a ocasião de haver reutilização de dados que dependem de consentimento e faculta ao usuário o direito de revogação (arts. 6º, inciso I, e 9º, § 2º), mas, para os dados sob a tutela do setor público, ou seja, que estão apoiados em competências legais, não há regras muito claras quanto ao reaproveitamento dessas informações.

O legislador precisa estar sempre vigilante no tocante à elaboração de normas internas que regulamentam as operações de transferência de informações, de modo que esses comandos sejam aptos a observar o plexo normativo superior que protege a autodeterminação informativa nas comunicações entre as diferentes bases de dados da Administração Pública.

Desse modo, os direitos fundamentais dos particulares não serão elididos pela concepção de supremacia do interesse público. Do contrário, seriam gerados efeitos indesejados, a exemplo de se criar uma interconexão generalizada de bases de dados públicas, sem qualquer parâmetro de proteção²⁰⁵.

Neste tópico foram revisitados alguns dos comandos legais e precedentes que buscaram firmar essa orientação.

3.3.1 Parâmetros fixados na ADI nº 6.649 e na ADPF nº 695

O art. 16, parágrafo único, do retromencionado Decreto nº 10.046/2019²⁰⁶,

²⁰⁴ WIMMER, 2021, p. 277.

²⁰⁵ *Ibid.*, p. 281.

²⁰⁶ BRASIL, ref. 117.

que instituiu o CBC, veda o uso da plataforma, ou o cruzamento desta com outras bases, “para a realização de tratamentos de dados que visem mapear ou explorar comportamentos individuais ou coletivos de cidadãos, sem o consentimento expresso, prévio e específico dos indivíduos afetados e sem a devida transparência da motivação e finalidade”. Com essa previsão, o legislador intentou proibir práticas abusivas no âmbito do compartilhamento de dados compartilhados pela Administração Pública federal, a exemplo do uso do *profiling*.

Adicionalmente, há de se mencionar que os dispositivos do decreto, sempre que fazem qualquer alusão à temática do tratamento de dados pessoais, apontam expressamente a observância da LGPD (v.g., art. 3º, inciso I).

Por outro lado, em que pesem (i) a iniciativa de coibir a utilização da ferramenta para as referidas atividades desviantes e (ii) as várias menções diretas à LGPD, a norma ainda previa outras regras que poderiam dar azo a severas violações da intimidade, a partir do compartilhamento massivo de dados pessoais.

Isso porque o CCGD, no exercício de suas atribuições regulamentares conferidas pelo referido diploma legal para categorizar, em diferentes níveis de proteção, os dados transferidos entre órgãos e entidades, recomendou que os dados pessoais fossem submetidos ao nível de *compartilhamento restrito*. À vista disso, conforme ressaltado no voto do Ministro Gilmar Mendes, quando do julgamento conjunto da ADI nº 6.649²⁰⁷ e da ADPF nº 695²⁰⁸, apesar de essa categoria almejar “impedir o acesso do público externo a dados cujo sigilo seja imprescindível à segurança da sociedade e do Estado”²⁰⁹, não obstaculiza “o livre fluxo das informações entre os diferentes órgãos que compõem o aparelho estatal”²¹⁰.

Dessa forma, essa classificação gerou uma preocupação que ia além da ideia de manutenção do sigilo, visto que o nível de *compartilhamento restrito*, apesar de manter a obstrução de acesso por qualquer indivíduo externo, ainda permite que os dados sejam livremente acessados por todos os órgãos e todas as entidades da Administração Pública federal. Assim, na visão da Corte, a orientação acaba por conferir “grave risco de malversação de dados pessoais e de violação da privacidade dos usuários do serviço público”²¹¹.

²⁰⁷ BRASIL, ref. 126.

²⁰⁸ BRASIL, ref. 127.

²⁰⁹ BRASIL, ref. 126, p. 32; BRASIL, ref. 127, p. 34.

²¹⁰ BRASIL, ref. 127, p. 34.

²¹¹ BRASIL, ref. 126, p. 32; BRASIL, ref. 127, p. 34.

O Tribunal alertou para o risco de se permitir um livre fluxo de dados que, apesar de aparentarem ser triviais, também podem estar ligados à privacidade do indivíduo. Nessa lógica, no voto condutor do Ministro Gilmar Mendes, é pontuado que o STF superou qualquer falsa ideia no sentido da possibilidade de existirem dados que, *a priori*, dispensariam a proteção constitucional.

Em referência ao posicionamento do Ministro Ricardo Lewandowski no julgamento da supracitada ADI nº 6.387, o Ministro decano indicou que a Corte passou a ter um novo olhar para essa questão. Isso porque informações que, em uma primeira leitura, possam parecer insignificantes – como o número de uma linha de celular – podem servir como “chave de identificação e de acesso a um universo de plataformas eletrônicas, como bancos, supermercados, serviços públicos e redes sociais, todas elas detentoras das mais variadas informações sobre o titular daquela linha telefônica”²¹².

Isso posto, à luz da nova orientação firmada pelo STF, não se leva em conta a natureza dos dados pessoais para uma efetiva salvaguarda da autodeterminação informativa, mas, sim, o “grau de sensibilidade das informações” e o “risco de malversação”, afastando-se qualquer “tentativa de abrandar o nível de proteção dispensado pela ordem jurídica sob o pretexto da simplicidade ou trivialidade das informações envolvidas”²¹³.

Tal consideração é de grande relevância, pois, a despeito de o diploma legal haver proibido o compartilhamento de dados sigilosos sob o domínio da autoridade tributária federal (art. 1º, § 2º), a RFB ainda pode transmitir elementos como as situações cadastrais no CPF e no CNPJ de contribuintes e dados sobre parcelamento e moratória de natureza global de débitos tributário, o que, na linha da mencionada conclusão do Ministro Lewandowski, pode desencadear um fornecimento desordenado de diversas outras informações sobre o contribuinte.

Todavia, é válida a ressalva de que, naquele julgamento, o Supremo não olvidou os avanços oriundos de medidas como as que foram introduzidas, no ordenamento jurídico brasileiro, com a norma apreciada. Contudo, por outro lado, muito se falou da importância de se ter uma máquina pública equipada com ferramentas que auxiliem no aprimoramento da gestão.

Destacou-se, nessa linha, a necessidade de o Estado não virar as costas para

²¹² BRASIL, ref. 199, p. 82.

²¹³ BRASIL, ref. 126.

o progresso tecnológico, devendo sempre o administrador público estar pautado pelo seu dever de eficiência. No entanto, esses avanços devem prestigiar as normas e os princípios plasmados na LGPD.

Um outro ponto muito explorado nesse aresto paradigmático diz respeito às distorções na composição do Comitê Central, haja vista que, segundo a redação do decreto, o órgão seria ocupado por servidores do Ministério da Fazenda, da Presidência da República, da Controladoria-Geral da União (CGU), da Advocacia-Geral da União (AGU) e do Instituto Nacional do Seguro Social (INSS), ou seja, exclusivamente por representantes da Administração Pública federal.

Essa configuração desbordava dos modelos criados em outros países, que contam com autoridades independentes para o monitoramento das operações de tratamento de dados pessoais. Nas palavras do Ministro Relator, essa composição tornava o Comitê uma “instituição com perfil insular, hostil a qualquer proposta de abertura democrática e de pluralização do debate”²¹⁴, uma vez que não permitiria a participação de representantes de outras instituições republicanas e de entidades da sociedade civil nos debates.

Diante dessas considerações, a Corte arredou qualquer interpretação da norma que possibilitasse o “amplo e irrestrito compartilhamento de dados pessoais entre órgãos e entidades da Administração Pública”²¹⁵. A partir de uma leitura do decreto presidencial alinhada com os valores constitucionais, afastou-se a possibilidade de os órgãos federais compartilharem informações concernentes aos atributos da personalidade ou qualidades próprias dos cidadãos.

Concluiu-se, nesse contexto, que uma declaração de inconstitucionalidade de toda a sistemática implementada pela norma geraria resultados ainda mais graves ao ordenamento jurídico brasileiro. Por conta disso, o STF conferiu interpretação conforme a Constituição Federal ao Decreto nº 10.046/2019, de modo a assegurar que o compartilhamento de dados entre órgãos e entidades da Administração Pública pressupõe a adoção dos seguintes critérios: eleição de propósitos legítimos, específicos e explícitos para o tratamento de dados; compatibilidade do tratamento com as finalidades informadas; e restrição do compartilhamento ao mínimo necessário para o atendimento do objetivo apontado.

Além disso, interpretou-se a norma no sentido de se determinar que o

²¹⁴ BRASIL, ref. 126, p. 84.

²¹⁵ BRASIL, ref. 126, p. 65.

repassa de dados entre órgãos públicos exige a observância do art. 23, inciso I, da LGPD²¹⁶. Esse dispositivo impõe uma regra de publicidade às situações em que a Administração compartilha ou tem acesso a banco de dados pessoais. Ainda segundo o aresto, a transgressão dolosa desse dever de publicidade, excetuadas as hipóteses constitucionais de sigilo, importa em responsabilização por ato de improbidade administrativa, nos termos do art. 11, inciso IV, da Lei nº 8.429, de 2 de junho de 1992, a Lei de Improbidade Administrativa (LIA)²¹⁷.

Complementarmente, a Suprema Corte impôs ao CCGD, no exercício de suas competências previstas no decreto presidencial, as seguintes incumbências²¹⁸:

3.1. prever mecanismos rigorosos de controle de acesso ao Cadastro Base do Cidadão, o qual será limitado a órgãos e entidades que comprovarem real necessidade de acesso aos dados pessoais nele reunidos. Nesse sentido, a permissão de acesso somente poderá ser concedida para o alcance de propósitos legítimos, específicos e explícitos, sendo limitada a informações que sejam indispensáveis ao atendimento do interesse público, nos termos do art. 7º, inciso III, e art. 23, caput e inciso I, da Lei 13.709/2018;

3.2. justificar de maneira formal, prévia e minudentemente, à luz dos postulados da proporcionalidade, da razoabilidade e dos princípios gerais de proteção da LGPD, tanto a necessidade de inclusão de novos dados pessoais na base integradora (art. 21, inciso VII) como a escolha das bases temáticas que comporão o Cadastro Base do Cidadão (art. 21, inciso VIII).

3.3. instituir medidas de segurança compatíveis com os princípios de proteção da LGPD, em especial a criação de sistema eletrônico de registro de acesso, para efeito de responsabilização em caso de abuso.

Por fim, declarou-se, com efeitos prospectivos, a inconstitucionalidade do art. 22 do decreto, preservando-se a composição vigente do CCGD pelo prazo de

²¹⁶ “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:

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;” BRASIL, ref. 22.

²¹⁷ “Art. 11. Constitui ato de improbidade administrativa que atenta contra os princípios da administração pública a ação ou omissão dolosa que viole os deveres de honestidade, de imparcialidade e de legalidade, caracterizada por uma das seguintes condutas:

[...]

IV - negar publicidade aos atos oficiais, exceto em razão de sua imprescindibilidade para a segurança da sociedade e do Estado ou de outras hipóteses instituídas em lei;”

BRASIL. **Lei nº 8.429, de 2 de junho de 1992**. Dispõe sobre as sanções aplicáveis em virtude da prática de atos de improbidade administrativa, de que trata o § 4º do art. 37 da Constituição Federal; e dá outras providências. Brasília: Presidência da República, [1992]. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8429.htm. Acesso em: 20 maio 2023.

²¹⁸ BRASIL, ref. 126.

sessenta dias, a contar da data de publicação da ata de julgamento. Esse período visava garantir que o Chefe do Poder Executivo tivesse tempo hábil para “(i) atribuir ao órgão um perfil independente e plural, aberto à participação efetiva de representantes de outras instituições democráticas; e (ii) conferir aos seus integrantes garantias mínimas contra influências indevidas”²¹⁹.

Do que se observa dos resultados desse julgamento é possível concluir que o STF lançou importantes luzes ao debate acerca dos parâmetros para a transmissão de dados. Esse precedente trouxe significativos avanços ao determinar que a política de transferência de dados deve (i) prever mecanismos rigorosos de controle de acesso à base de dados e limitar o uso aos órgãos e às entidades que comprovarem a real necessidade de obtenção dos dados pessoais nela reunidos, (ii) exigir a comprovação de “propósitos legítimos, específicos e explícitos”²²⁰, restringindo o uso apenas às informações indispensáveis ao atendimento do interesse público, (iii) demandar, para a inclusão de informações e para a escolha de bases temáticas, uma justificativa formal, prévia e minudente, fundamentada na proporcionalidade, na razoabilidade e nos princípios gerais de proteção da LGPD, (iv) impor meios de segurança orientados por princípios da LGPD, notadamente a implementação de uma sistema de registro de acesso para aferir possíveis responsabilizações dos agentes públicos em casos de abuso, e (v) exigir que o Chefe do Executivo, no bojo de sua competência para regular as atribuições do órgão fiscalizador, implemente uma composição plural e independente, que permita a participação de representantes oriundos de instituições democráticas de fora da Administração Pública e que esses membros possuam as garantias mínimas contra influências indevidas.

É inegável que foram definidos, nesse julgado, relevantes contornos para a atuação dos agentes públicos brasileiros, inclusive para os representantes dos órgãos tributários. Essas premissas permitem orientar a atividade de fiscalização sob o prisma das normas de proteção de dados pessoais. O Fisco, como detentor de muitas dessas informações, deve cumprir os comandos firmados pela Corte, para que possa haver um efetivo controle das informações divulgadas pelas autoridades tributárias.

Por oportuno, é válido mencionar que, à luz desse julgamento e em meio à já

²¹⁹ BRASIL, ref. 126, p. 6.

²²⁰ BRASIL, ref. 126, p. 2.

anunciada dificuldade de se implementar algumas dessas regras de proteção de usuários/contribuintes, o *compliance* de dados poderia servir como um importante instrumento para o propósito de se assegurar a efetividade de tais comandos.

Como bem ensina a professora Ana Frazão, o *compliance* pode ser definido como “um conjunto de ações a serem adotadas no ambiente corporativo para que se reforce a anuência da empresa à legislação vigente, de modo a prevenir a ocorrência de infrações ou, já tendo ocorrido o ilícito, propiciar o imediato retorno ao contexto de normalidade e legalidade”. Trata-se de ideia voltada para a difusão de boas práticas de respeito às normas jurídicas e éticas, que, quando transferidas para o universo dos dados, visam assegurar, precipuamente, a salvaguarda dos direitos de seus titulares²²¹.

Considerando as diretrizes fixadas, no sentido de promoção de um diálogo plural, pautado na finalidade e necessidade, algumas ferramentas de adequação poderiam ser pensadas para o setor público, notadamente para a Administração Tributária.

Não por outro motivo que o art. 32 da LGPD previu a possibilidade de a autoridade nacional “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”. A iniciativa estimula a implementação da medida no tratamento de dados pelo setor público.

3.3.2 Balizas para o compartilhamento de procedimentos fiscalizatórios com os órgãos de persecução penal

No julgamento do mencionado Tema 990 da repercussão geral – RE nº 1.055.941/SP²²² –, o STF definiu alguns quesitos para a disponibilização de dados sob o domínio da RFB e da Unidade de Inteligência Financeira (UIF) – atual Conselho de Controle de Atividades Financeiras (Coaf) – ao Ministério Público. No contexto desse debate, foram investigados os aspectos do procedimento de fornecimento de informações por esses órgãos.

²²¹ FRAZÃO, Ana. Propósitos, desafios e parâmetros gerais dos programas de *compliance* e das políticas de proteção de dados. In: FRAZÃO, Ana; CUEVA, Ricardo Villas Bôas (Orgs.). **Compliance e Política de Proteção de Dados**. São Paulo: Thomson Reuters Brasil, 2021. p. 33-62. p. 36-37.

²²² BRASIL, ref. 91.

Como cediço, examinava-se, naquela assentada, a constitucionalidade do compartilhamento, sem decisão judicial, dos dados bancários e fiscais dos cidadãos, coletados no exercício legítimo da atividade fiscalizadora dos órgãos administrativos do Poder Público, com o *Parquet* para fins penais. No decorrer das discussões ali travadas, discorreu-se, inicialmente, sobre os papéis e as diferentes fases que envolvem os expedientes de análise e de comunicação da UIF, órgão responsável por fiscalizar, por meio do intercâmbio de informações, operações financeiras e tributárias com a finalidade de prevenção a crimes como lavagem de dinheiro.

A UIF realiza um trabalho de inteligência financeira e seus relatórios são elaborados com base nas informações recebidas pelos comunicantes: o órgão recebe, processa, armazena e, caso constate alguma atividade suspeita ou movimentações em dinheiro vivo acima do valor máximo legalmente estabelecido, dissemina os dados às autoridades competentes relevantes.

Os comunicantes são as pessoas físicas e jurídicas dos chamados *setores obrigados*, que, por determinação legal, estão sujeitas às obrigações de identificação, registro e comunicação das operações financeiras dos clientes. À luz do art. 9º da Lei nº 9.613/1998²²³, que dispõe sobre medidas preventivas, no sistema financeiro, contra os crimes de lavagem ou ocultação de bens, direitos e valores, são exemplos de negócios enquadrados nessa definição: instituições financeiras, seguradoras, corretoras de valores, joalherias, comércios de bens de luxo, juntas comerciais, cartórios etc.

Portanto, a UIF funciona como um filtro na comunicação entre o setor financeiro e as entidades comunicantes. Não compete à unidade fiscalizadora acessar ou requisitar as contas bancárias para buscar operações suspeitas²²⁴, mas, sim, avaliar o risco das transações informadas pelas entidades.

Como bem delineado no *leading case*, o modelo brasileiro segue o padrão estabelecido internacionalmente de prevenção à lavagem de dinheiro e combate ao

²²³ BRASIL. **Lei nº 9.613, de 3 de março de 1998**. Dispõe sobre os crimes de “lavagem” ou ocultação de bens, direitos e valores; a prevenção da utilização do sistema financeiro para os ilícitos previstos nesta Lei; cria o Conselho de Controle de Atividades Financeiras – COAF, e dá outras providências. Brasília: Presidência da República, [1998]. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9613.htm. Acesso em: 20 maio 2023.

²²⁴ Em seu voto, o Ministro Dias Toffoli destaca a “absoluta e intransponível impossibilidade da geração de RIF [Relatório de Inteligência Financeira] por encomenda (*fishing expedition*) contra cidadãos que não estejam sob investigação criminal de qualquer natureza ou em relação aos quais não haja alerta já emitido de ofício pela unidade de inteligência com fundamento na análise de informações contidas em sua base de dados”. BRASIL, ref. 91, p. 44.

financiamento do terrorismo²²⁵. Para alcançar esse objetivo, utiliza-se uma estratégia de supervisão rigorosa de operações em diversos setores da economia, o que, inevitavelmente, envolve o acesso a uma grande quantidade de dados pessoais.

Por outro lado, a questão torna-se ainda mais sensível ao se verificar o intercâmbio de informações da RFB com as instituições financeiras. A operação é regulamentada pela Instrução Normativa SRF nº 165/2002²²⁶, que aprovou a criação do Programa de Atendimento à Requisição de Informações sobre Movimentação Financeira (PA-RMF).

Trata-se de ferramenta que permite a transmissão das informações requisitadas nos termos do Decreto nº 3.724, de 10 de janeiro de 2001²²⁷, que regulamenta o art. 6º da Lei Complementar nº 105/2001. Esse último dispositivo exige a instauração de processo administrativo ou que haja um procedimento fiscal em curso para que as autoridades e os agentes fiscais possam examinar documentos, livros e registros de instituições financeiras. A norma também determina que tais exames devam ser considerados indispensáveis pela autoridade administrativa.

Munido dessas informações sigilosas, o Fisco tem o dever legal de comunicar o órgão acusatório sobre algum indício de prática de crimes, o que se dá pela formalização de Representação Fiscal para Fins Penais (RFFP) ou de Representação para Fins Penais (RFP). Nesse particular, foi travado, na Corte, um extenso debate em relação à seguinte pergunta, sintetizada no voto do Ministro Relator²²⁸:

²²⁵ Nesse particular, destaca-se o trabalho do Grupo de Ação Financeira (GAFI), criado em 1989. O GAFI promove políticas intergovernamentais de cooperação voltadas à proteção do sistema financeiro e da economia em geral contra os referidos ilícitos. Disponível em: <https://www.gov.br/susep/pt-br/assuntos/cidadao/pldftp/o-grupo-de-acao-financeira-gafi-fatf>. Acesso em: 6 maio 2023.

²²⁶ BRASIL. Secretaria Especial da Receita Federal do Brasil. **Instrução Normativa SRF nº 165, 10 de junho de 2002**. Aprova o Programa de Atendimento à Requisição de Informações sobre Movimentação Financeira (PA-RMF). Diário Oficial da União, Brasília, DF, 12 jun. 2002, seção 1, p. 18. Disponível em: <http://normas.receita.fazenda.gov.br/sijut2consulta/link.action?idAto=15017&visao=anotado>. Acesso em: 24 maio 2023.

²²⁷ BRASIL. **Decreto nº 3.724, de 10 de janeiro de 2001**. Regulamenta o art. 6º da Lei Complementar nº 105, de 10 de janeiro de 2001, relativamente à requisição, acesso e uso, pela Secretaria da Receita Federal, de informações referentes a operações e serviços das instituições financeiras e das entidades a elas equiparadas. Brasília: Presidência da República, [2001]. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto/2001/d3724.htm#:~:text=DECRETO%20N%C2%BA%203.724%2C%20DE%2010%20DE%20JANEIRO%20DE%202001.&text=Regulamenta%20o%20art.%20das%20entidades%20a%20elas%20equiparadas. Acesso em: 24 maio 2023.

²²⁸ BRASIL, ref. 91, p. 67.

[C]onsiderado o dever legal da autoridade fiscal de formalizar a representação fiscal para fins penais (RFFP) ou, nos crimes conexos, a representação para fins penais (RFP), quais informações do contribuinte podem ser transferidas ao Ministério Público, para fins de persecução penal, sem afetar a higidez dos sigilos fiscal e bancário, assegurados constitucionalmente nos incisos X e XII do art. 5º da Constituição Federal?

Em primeiro lugar, registrou-se que, consoante o disposto no art. 198 do CTN, o fornecimento de informações fiscais dentro da Administração Pública precisa seguir o devido processo administrativo, com a garantia de registro de todas as etapas do procedimento e da fundamentação da motivação da autoridade solicitante.

Considerou-se, ainda, que o art. 198, § 1º, inciso II, do CTN excepciona o sigilo na hipótese de “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”, bem como que se objetive “investigar o sujeito passivo a que se refere a informação, por prática de infração administrativa”²²⁹. Fora essa situação, exige-se requisição de autoridade judiciária no interesse da justiça (art. 198, § 1º, inciso I).

Em relação ao art. 198, § 3º, do CTN, o Ministro Dias Toffoli destacou que, apesar de o dispositivo ressaltar a vedação de divulgação das informações relativas à RFFP (inciso I), a autorização “não respalda a interpretação de ser possível instruir a RFFP com documentos do contribuinte investigado que contenham informações sigilosas suas e de terceiros, como é o caso da declaração de ajuste anual e dos extratos bancários”²³⁰. Isso porque a Representação Fiscal para Fins Penais, formalizada em autos apartados, não se confundiria com o Processo Administrativo Fiscal (PAF), este destinado à apuração do crédito tributário.

Demais disso, também foi feita a distinção entre a representação em si e os documentos que a instruem. Citando o exemplo de uma RFFP que constate omissão de receita a partir de informações extraídas de extratos bancários, ponderou o julgador que a representação não poderia ser instruída com esses dados.

Nessa linha de ideias, seria lícito que o procedimento possuísse dados pinçados de documentos sigilosos obtidos pelo Fisco, mas não poderiam constar da RFFP encaminhada ao *Parquet* informações acobertadas pelo sigilo fiscal que não tivessem “qualquer pertinência com a descrição de fato suspeito ou ao qual se

²²⁹ BRASIL, 1966.

²³⁰ BRASIL, ref. 91, p. 70.

atribua, em tese, o caráter de ilícito”²³¹. Com base nesse entendimento, concluiu o Ministro Toffoli que os dispositivos infralegais que permitiam que a representação fosse instruída com as declarações ou escriturações apresentadas à RFB relacionadas ao lançamento e documentos com indícios de irregularidades apreendidos no curso da ação fiscal (Portaria RFB nº 1.750/2018²³²) estariam “em descompasso com as normas legais (art. 198, CTN, art. 83 da Lei 9.430/1996 e art. 1º, § 3º, IV, da LC nº 105/01) e constitucionais que garantem o direito à intimidade e à inviolabilidade de dados (art. 5º, X e XII, da CF)”²³³.

Tal solução seria de grande relevância prática, porque, segundo o Ministro Relator, observava-se a praxe de a RFB repassar, por intermédio da RFFP, a cópia integral do PAF ao Ministério Público, a qual continha dados financeiros, de terceiros e estranhos aos fatos criminosos apurados na representação. Assim, buscava-se garantir que a operação seguisse rigorosamente as regras de compartilhamento dentro dos limites da persecução criminal, de modo a se evitar o fornecimento de dados pessoais estranhos à apuração do ilícito penal e que dariam ensejo à violação à garantia da privacidade.

No entanto, prevaleceu a corrente inaugurada pelo Ministro Alexandre de Moraes no sentido da constitucionalidade do compartilhamento da íntegra do procedimento. Em suas considerações, o Ministro ressaltou que, nos crimes tributários, o titular da ação penal pública está condicionado ao término da atuação da Receita Federal. Dessa forma, o Ministério Público somente poderia oferecer denúncia e obter eventual condenação, em relação a esses crimes, se comprovasse “a existência de lançamento definitivo de tributo contra o acusado (materialidade do delito)”²³⁴.

Nesse sentido, a mera alegação de existência de lançamento definitivo de tributo seria insuficiente, sendo necessária a demonstração de sua regularidade

²³¹ BRASIL, ref. 91, p. 71.

²³² BRASIL. Secretaria Especial da Receita Federal do Brasil. **Portaria RFB nº 1.750, de 12 de novembro de 2018**. Dispõe sobre representação fiscal para fins penais referente a crimes contra a ordem tributária, contra a Previdência Social, e de contrabando ou descaminho, sobre representação para fins penais referente a crimes contra a Administração Pública Federal, em detrimento da Fazenda Nacional ou contra administração pública estrangeira, de falsidade de títulos, papéis e documentos públicos e de “lavagem” ou ocultação de bens, direitos e valores, e sobre representação referente a atos de improbidade administrativa. Diário Oficial da União, Brasília, DF, 14 nov. 2018, seção 1, p. 57. Disponível em: <http://normas.receita.fazenda.gov.br/sijut2consulta/link.action?idAto=96434>. Acesso em: 18 maio 2023.

²³³ BRASIL, ref. 91, p. 77-78.

²³⁴ BRASIL, ref. 91, p. 194.

formal, com a “comprovação do regular lançamento definitivo de tributo contra o acusado após o devido procedimento de fiscalização com todas as exigências legais”²³⁵, e a evidência material da existência de irregularidade tributária por parte do contribuinte.

Conforme aduziu o Ministro Alexandre, essa exigência seria essencial porque, visando garantir o devido processo legal, a ampla defesa e o contraditório, os termos do lançamento definitivo do tributo pela RFB – que comprovam a materialidade do crime – poderiam ser novamente impugnados em juízo.

Desse modo, argumentou-se que o regular lançamento definitivo do tributo, como “elemento necessário e essencial para o oferecimento da denúncia nos crimes materiais contra a ordem tributária”²³⁶, precisa obrigatoriamente estar respaldado pelo material probatório constante no procedimento de fiscalização. Com base nesse raciocínio, pontuou o Ministro que seria, inclusive, inepta a acusação que não aguardasse o término do procedimento com a conclusão pelo lançamento definitivo do tributo, isto é, com a prova da materialidade da infração penal tributária. Assim, complementou que “todas as informações e dados constantes no procedimento de fiscalização são provas lícitas, pois obtidas pela Receita Federal em absoluto respeito ao direito material”²³⁷.

O Ministro Dias Toffoli, com a ressalva de seu entendimento quanto ao envio de dados não relacionados à apuração do ilícito penal, acatou a conclusão do Ministro Alexandre de Moraes no sentido da possibilidade de envio da íntegra do PAF ao *Parquet*, “sem a obrigatoriedade de prévia autorização judicial, devendo ser resguardado o sigilo das informações em procedimentos formalmente instaurados e sujeitos a posterior controle jurisdicional”²³⁸. Esse compartilhamento deve, nos termos da tese fixada, “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”²³⁹.

3.4 Penalidades aplicáveis aos agentes públicos

²³⁵ BRASIL, ref. 91, p. 194.

²³⁶ BRASIL, ref. 91, p. 194.

²³⁷ BRASIL, ref. 91, p. 194.

²³⁸ BRASIL, ref. 91, p. 529.

²³⁹ BRASIL, ref. 91, p. 529.

Além das normas e dos princípios que orientam a atividade de transmissão e coleta, os servidores públicos estão sujeitos a penalidades de natureza penal, administrativa e civil, caso violem a confidencialidade.

No Código Penal brasileiro²⁴⁰, o art. 325 dispõe sobre o crime de “violação de sigilo funcional”. Segundo esse dispositivo, o ato de “revelar fato de que tem ciência em razão do cargo e que deva permanecer em segredo, ou facilitar-lhe a revelação” constitui delito, cuja pena é de detenção, de seis meses a dois anos, ou multa, se o fato não constituir crime mais grave.

Segundo o § 1º desse mesmo artigo, quem “permite ou facilita, mediante atribuição, fornecimento e empréstimo de senha ou qualquer outra forma, o acesso de pessoas não autorizadas a sistemas de informações ou banco de dados da Administração Pública” ou “se utiliza, indevidamente, do acesso restrito” também incorre nas referidas penas. Ademais, se a ação ou omissão do agente resultar em algum dano à Administração Pública ou a outrem, a pena será de reclusão, de dois a seis anos, e multa.

No âmbito administrativo, conforme aludido no tópico sobre o sigilo fiscal, o art. 132, inciso IX, da Lei nº 8.112/1990 prevê como hipótese da penalidade de demissão a “revelação de segredo do qual se apropriou em razão do cargo”²⁴¹. Tal sanção encontra-se expressamente indicada no art. 6º da mencionada Portaria RFB nº 2.344/2011, que regulamenta o acesso a informações protegidas por sigilo fiscal, constantes de sistemas informatizados da RFB²⁴².

Demais disso, essa violação também configura ato de improbidade administrativa, nos termos do art. 11, inciso III, da LIA²⁴³.

Além dessas penalidades, o servidor que violar o sigilo fiscal também poderá responder judicialmente, em ação de reparação de danos morais e materiais. Nesse particular, embora os dados cadastrais não sejam protegidos pela cláusula de sigilo,

²⁴⁰ BRASIL. **Decreto-lei nº 2.848, de 7 de dezembro de 1940**. Código Penal. Brasília: Presidência da República, [1940]. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 6 maio 2023.

²⁴¹ BRASIL, 1991.

²⁴² BRASIL, ref. 69.

²⁴³ “Art. 11. Constitui ato de improbidade administrativa que atenta contra os princípios da administração pública a ação ou omissão dolosa que viole os deveres de honestidade, de imparcialidade e de legalidade, caracterizada por uma das seguintes condutas:

[...]

III - revelar fato ou circunstância de que tem ciência em razão das atribuições e que deva permanecer em segredo, propiciando beneficiamento por informação privilegiada ou colocando em risco a segurança da sociedade e do Estado;”

BRASIL, 1992.

há a necessidade de se observar as normas legais e regulamentares, bem como o dever funcional de sigilo sobre os assuntos da Administração Pública, à luz do art. 116, incisos III e VIII, da Lei nº 8.112/1990²⁴⁴.

Da leitura dessas regras, juntamente com as demais normas da Administração Tributária, nota-se que o agente público também não pode acessar imotivadamente ou fornecer dados cadastrais a quem não estiver legalmente autorizado, sob pena de descumprimento de seu dever funcional e de violação às normas que regem a sua atuação.

A partir da análise desses dispositivos, verifica-se que a responsabilização cível, criminal e administrativa vai além da LGPD. Isso porque o setor público dispõe de mecanismos de responsabilização de todos os seus agentes inseridos no regime jurídico dos servidores públicos.

Todavia, a LGPD também delinea algumas situações de responsabilização: o art. 42 dessa lei trata da hipótese de reparação de danos no caso de o controlador ou o operador, “causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais”, em razão do exercício de atividade de tratamento de dados pessoais. Assim como reconheceu o STF no julgamento da referida ADI nº 6.649, a regra é aplicável ao âmbito do Poder Público, com as necessárias adaptações.

Uma ressalva para a transposição desse regramento ao setor público é observada na tese firmada no julgamento do RE nº 1.027.633/SP, representativo do Tema 940 da repercussão geral. Naquela oportunidade, a Corte fixou o entendimento de que “a ação por danos causados por agente público deve ser ajuizada contra o Estado ou a pessoa jurídica de direito privado prestadora de serviço público”²⁴⁵. O autor do ato, por sua vez, é parte ilegítima para essa ação, mas fica assegurado o direito de regresso contra o responsável nas situações de dolo ou culpa.

Nessa perspectiva, a LGPD não deve ser esquecida ao se investigar as ações daqueles servidores que realizam o tratamento de dados tributários, bem como em qualquer operação de utilização de dados pessoais pelo Estado²⁴⁶. Em verdade, em

²⁴⁴ BRASIL, 1991.

²⁴⁵ BRASIL. Supremo Tribunal Federal. **RE nº 1.027.633/SP**. Rel. Min. Marco Aurélio. Brasília, DF, Plenário, j. 14/8/2019, *DJ* 6/12/2019. p. 14. Disponível em: <https://jurisprudencia.stf.jus.br/pages/search/sjur416502/false>. Acesso em: 6 out. 2023.

²⁴⁶ Cf. WIMMER, 2021.

razão da incipiência da implementação da norma, é cedo para cravar o seu alcance dentro desse campo.

Fato é que a LGPD delegou à autoridade nacional a tarefa de elaborar “informe com medidas cabíveis para fazer cessar a violação”, quando houver infração à lei decorrente do tratamento de dados pessoais por órgãos públicos (art. 31). Ademais, nos termos do art. 55-J, inciso XXII, compete à ANPD “comunicar aos órgãos de controle interno o descumprimento do disposto nesta Lei por órgãos e entidades da administração pública federal”²⁴⁷. Dessa forma, conclui-se que o legislador buscou abarcar, no âmbito da competência da ANPD, as atribuições para a fiscalização das atividades dos órgãos públicos, inclusive daqueles vinculados à Receita Federal.

3.5 Diretrizes internacionais e a experiência comparada

A preocupação com o crescimento das operações de governança envolvendo dados e novas tecnologias não escapou aos olhos das grandes organizações internacionais. Nesse sentido, a OCDE, empenhada em desenvolver estudos voltados às boas práticas no âmbito da Economia Digital, publicou, em 2019, o relatório “*The Path to Becoming a Data-Driven Public Sector*”²⁴⁸.

No documento, é ressaltado que, a despeito dos significativos avanços no fortalecimento da capacidade de utilização estratégica de dados para a melhoria de políticas públicas, prestação de serviços e gerenciamento do desempenho da atividade estatal, esse mecanismo ainda não era visto como um meio fundamental para a criação de valor público nessas operações.

Dessa maneira, com base nos últimos trabalhos da organização direcionados ao exame do papel dos dados na sociedade e na economia, o relatório propõe um modelo para analisar o “setor público movido a dados” (*Data-Driven Public Sector – DDPS*)²⁴⁹, de forma a maximizar “as oportunidades oferecidas pelos dados no

²⁴⁷ BRASIL, ref. 22.

²⁴⁸ OCDE. **The Path to Becoming a Data-Driven Public Sector**. Paris: OECD Publishing, 2019. Disponível em: <https://www.oecd.org/gov/the-path-to-becoming-a-data-driven-public-sector-059814a7-en.htm>. Acesso em: 24 jul. 2023.

²⁴⁹ Cf. VAN OOIJEN, Charlotte; UBALDI, Barbara; WELBY, Benjamin. **A data-driven public sector: Enabling the strategic use of data for productive, inclusive and trustworthy governance**. OECD Working Papers on Public Governance. Paris: OECD Publishing, n. 33, 2019. Disponível em: https://www.oecd-ilibrary.org/governance/a-data-driven-public-sector_09ab162c-en. Acesso em: 24 jul. 2023.

século XXI” (tradução nossa)²⁵⁰. Com isso, propõe-se que um sistema verdadeiramente movido a dados precisa (i) reconhecer os dados como ativos estratégicos fundamentais, com seu valor bem definido e seu impacto previamente estipulado, (ii) refletir os esforços para remover as barreiras para gerenciar, compartilhar e reutilizar as informações, (iii) aplicar esses subsídios para transformar o *design*, a entrega e o monitoramento de políticas públicas e de serviços e (iv) valorizar o empenho para fornecer dados abertamente, bem assim o uso de informações entre e dentro das organizações da Administração Pública.

No trabalho é ressaltada a necessidade de se adotar uma perspectiva integral de governo (*whole-of-government approach*) ao se pensar nesse modelo, sopesando-se a melhoria nos serviços prestados com a transparência e a confiabilidade no uso dos dados. Para tanto, o debate é dividido em três grandes áreas de discussão.

Primeiramente, destaca-se justamente a questão de os países desenvolverem um *modelo de governança digital* confiável e eficiente, o que ocorreria pela definição precisa sobre a finalidade da atividade estatal e do desenvolvimento de uma “estrutura comum” a ser implementada nos mais variados Estados do globo. Nessa linha, seriam componentes dessa estrutura²⁵¹:

- * Garantir a liderança e a visão para assegurar o direcionamento estratégico e o propósito da conversa orientada por dados em todo o setor público;
- * Incentivar a implementação coerente dessa estrutura do setor público orientada por dados em todo o governo e em organizações individuais;
- * Estabelecer ou revisar regras, leis, diretrizes e padrões associados aos dados;
- * Garantir a existência de uma arquitetura de dados que reflita padrões, interoperabilidade e semântica em toda a geração, coleta, armazenamento e processamento de dados;
- * Desenvolver a infraestrutura de dados necessária para apoiar a publicação, o compartilhamento e a reutilização de dados (tradução nossa).

Um segundo passo seria a aplicação de dados para gerar um *valor público* a

²⁵⁰ No original: “Building on previous OECD work about the role of data in society and the economy, this report proposes a model for understanding the ‘data driven public sector’ (DDPS) that will maximise the opportunities provided by twenty-first century data”. OCDE, ref. 248.

²⁵¹ No original: “securing the leadership and vision to ensure strategic direction and purpose for the data-driven conversation throughout the public sector; Encouraging the coherent implementation of this data-driven public sector framework across government as a whole and within individual organisations; Putting in place, or revisiting, rules, laws, guidelines and standards associated with data; Ensuring the existence of a data architecture that reflects standards, interoperability and semantics throughout the generation, collection, storage and processing of data; Developing the necessary data infrastructure to support the publication, sharing and re-use of data”. OCDE, ref. 248.

partir das seguintes atividades: (i) antecipação e previsão de mudanças e planejamento de políticas e de planos de intervenção; (ii) informação e aprimoramento da implementação de medidas, bem como da responsividade dos governos e da oferta de serviços públicos; e (iii) avaliação e monitoramento de impactos, decisões e desempenho.

Por fim, na terceira seção, investiga-se o papel dos dados na formação da *confiança pública*. Nesse particular, é pontuado que um objetivo do relatório é o de desafiar os governos a adotarem uma “abordagem ética” para orientar as escolhas dos cidadãos, fomentar a proteção da privacidade e a transparência, estimular soluções que ajudem a informar os usuários acerca do consentimento para o uso de seus dados e equilibrar a segurança dos serviços públicos com a minoração dos riscos de quebra de segurança sem impedir o desenvolvimento dessas ferramentas.

No que concerne à criação de uma estrutura de governança de dados, a OCDE busca propor um modelo holístico. Nessa linha, pondera-se que a idealização de um padrão contribuiria para a implementação eficaz de iniciativas de coleta, compartilhamento e acesso a dados entre diferentes setores da Administração.

É mencionado, nesse ponto, o sistema holandês, no qual se implementou o *Standard Business Reporting* (SBR), medida que “reduziu o ônus imposto às empresas no fornecimento de informações comerciais às autoridades locais e aos bancos”. Com o SBR, a Holanda conta com uma estrutura de governança de dados público-privada compartilhada, supervisionada por um Comitê Diretor do setor público, que define as metas e o programa de trabalho. Nessa sistemática, também se criou uma plataforma, pela qual os atores dos setores público e privado podem monitorar e oferecer consultoria sobre a implementação do programa²⁵². Dessa forma, o sistema holandês tratou de padronizar e, assim, simplificar o tratamento de dados pelo Poder Público.

Ainda em relação ao modelo a ser pensado, o estudo traz uma ponderação concernente à privacidade e ao consentimento pelo usuário. O texto pontua que os países têm estabelecido requisitos formais voltados à proteção do cidadão e à transparência de informações como os dados a serem utilizados, as organizações públicas envolvidas e as finalidades de cada operação.

Nessa via, foram pensados alguns valores com o objetivo de se desenvolver

²⁵² OCDE, ref. 248.

um “conjunto comum de princípios” e, assim, contribuir para a promoção de uma cultura de observância de diretrizes éticas nas operações digitais. Com isso, liderado pela Holanda, o Grupo Temático sobre o DDPS definiu quais seriam as condutas ideais a serem implementadas (*data ethics guidelines*).

Em primeiro lugar, estipulou-se que o uso e a coleta dos dados em um DDPS precisam ter um valor público, isto é, um interesse coletivo subjacente, o que somente ocorreria com o fortalecimento das instituições democráticas e do Estado de Direito. Assim, segundo o relatório, o tratamento com base em diretrizes éticas deve ser a regra.

Também se exigiu que haja clareza sobre a finalidade do uso de algum dado específico. Nesse sentido, “[t]odas as partes do ciclo de valor dos dados devem entender claramente o objetivo, que deve ser articulado *ex ante* de cada uso de dados e em cada estágio” (tradução nossa)²⁵³. É necessário, ainda, definir os limites de uso, de modo a se permitir apenas a utilização do essencial para a conclusão das diligências. Dessa forma, ressalta-se a importância da utilização dos dados com integridade, sem que o Poder Público incorra em abusos.

Fala-se, ademais, da utilização responsável dos dados para que se possa ganhar a confiança do usuário. A responsabilidade não se refere apenas à divulgação acerca do tratamento e da publicização, mas também à “transparência das atividades do governo e à segurança digital suficientemente forte para proteger os dados mantidos pelo governo” (tradução nossa)²⁵⁴. Em outras palavras, exige-se que o Estado ateste a efetividade dos mecanismos de segurança para com os dados sob sua custódia.

Por último, destaca-se a importância de se capacitar os cidadãos como forma de conferir mais controle sobre seus dados pessoais. Nessa senda, é pontuada a necessidade de se reconhecer os direitos de ser informado, de acessar, de modificar, de excluir e restringir informações, de transferir dados, de fazer objeções etc. Esse processo visa evitar a discriminação e apoiar a inclusão.

Da mesma forma, é citado o dever de tratar as informações de forma responsável e evitar dados tendenciosos. Por conseguinte, pondera-se que os

²⁵³ No original: “All parties of the data value cycle should plainly understand the goal, which should be articulated *ex ante*, of every use of data and at every stage”. OCDE, ref. 248.

²⁵⁴ No original: “Accountability is not just about disclosing how personal data are being handled and publishing public data, but also about being transparent with government activities and having strong enough digital security to protect government-held data”. OCDE, ref. 248.

funcionários públicos precisam estar equipados com as habilidades técnicas adequadas para poder identificar erros e situações potencialmente prejudiciais.

Em conclusão, observa-se que, com vistas a “extrair e agregar valor aos dados, os governos devem criar uma base sólida de governança de dados”, a qual “deve permitir a implementação coerente de políticas e definir ambientes confiáveis e seguros para o compartilhamento ético e a reutilização de dados” (tradução nossa)²⁵⁵.

No que tange aos desafios elencados, é ressaltado que não há uma solução simples ou única. Em verdade, as autoridades precisariam desenvolver metodologias que refletissem a realidade local, mas orientadas pelo valor público conferido aos dados e pela transparência em relação à finalidade do tratamento e aos benefícios esperados para a sociedade.

A informação é importante para demonstrar o caráter não vinculante das diretrizes firmadas pela OCDE. Em verdade, em que pese ter sido levantada a necessidade de se pensar em um padrão de DDPS, o documento mais se assemelha a um manual de boas práticas, com recomendações gerais ao setor público no âmbito digital. Contudo, para uma aplicação de viés pragmático da metodologia, faz-se imprescindível investigar as especificidades de cada sistema interno.

À vista disso e com base nos objetivos desta pesquisa, serão abordados, a seguir, alguns dos casos do direito comparado em que se discutiu a aplicação de políticas de proteção de dados para questões tributárias. As repercussões desses exemplos relatados são relevantes para que se possa pensar em parâmetros para o direito brasileiro.

3.5.1 As alterações no Código Tributário alemão

No direito alemão, foram travados significativos debates legislativos acerca da aplicação das normas de proteção de dados à esfera tributária. Por meio da *Gesetz zur Änderung des Bundesversorgungsgesetzes und anderer Vorschriften*, lei de 2017, foram introduzidas várias obrigações acessórias no Código Tributário alemão

²⁵⁵ No original: “In order to extract and deliver value from data, governments must build a solid data governance foundation. Such a foundation should allow coherent policy implementation, and define trustworthy and safe environments for the ethical sharing and reuse of data”. OCDE, ref. 248.

(*Abgabenordnung* – AO) relativas à conformidade com o RGPD (§§ 32a-32f).

No entanto, a relação entre o Código Tributário alemão e as normas de proteção de dados ainda se apresentava confusa em alguns aspectos. Isso porque, entre os dispositivos acrescentados, houve expressa previsão de não aplicação do AO àquilo que o RGPD diretamente regula. Como explica Roman Seer, isso representaria um equívoco, porque a norma tributária alemã preenche as cláusulas abertas do regulamento de proteção de dados. Afinal, trata-se de regramento específico do direito alemão voltado para as obrigações tributárias²⁵⁶.

O § 2^a, par. 5, n. 2, da AO, por sua vez, amplia “o âmbito de aplicação do RGPD para o nível nacional, abrangendo, entre outros, as corporações, as associações com ou sem capacidade jurídica e as universalidades de bens”. Também com base nos ensinamentos de Roman Seer, “o dispositivo não esclarece se a partir de agora há um direito autônomo de proteção de dados fiscais, o qual impõe a aplicação do RGPD em conjunto com a AO apenas sobre os impostos abarcados pelas normas da UE” ou se todos os tributos estariam abarcados²⁵⁷.

No que concerne ao tratamento de dados pela Administração Tributária, as alterações no diploma legal alemão instituíram regramentos tanto para a finalidade específica da operação como para um tratamento subsecutivo (AO, §§ 29b e 29c)²⁵⁸.

Orientado pelo princípio da finalidade, o § 29b versa sobre o tratamento de dados pessoais apenas para os propósitos pelos quais eles forem capturados. Por sua vez, o § 29c dispõe sobre o *tratamento posterior* dos dados, isto é, para um objetivo diferente do que deu ensejo à coleta inicial.

Todavia, o referido dispositivo possibilita o tratamento posterior somente em seis situações: (i) se o tratamento se destinar a facilitar um processo administrativo fiscal, um procedimento de fiscalização ou um processo judicial tributário ou penal-tributário; (ii) caso estejam reunidas as condições legais que permitam a divulgação desses dados nos termos do item 4 ou 5 do art. 30 do Código (quebra de sigilo fiscal nas ocasiões de auxílio a procedimentos sobre crimes tributários ou existência de interesse público prevalente) ou se for necessário verificar se essas condições estão

²⁵⁶ SEER, 2020, p. 20-47 .

²⁵⁷ *Ibid.*, p. 30-31.

²⁵⁸ ALEMANHA. Bundesministerium der Finanzen. **The Fiscal Code of Germany**. Fiscal Code of Germany in the version promulgated on 1 October 2002 (Federal Law Gazette [Bundesgesetzblatt] I p. 3866; 2003 I p. 61), last amended by Article 17 of the Act of 17 July 2017 (Federal Law Gazette I p. 2541). Disponível em: https://www.gesetze-im-internet.de/englisch_ao. Acesso em: 20 maio 2023.

reunidas; (iii) quando for evidente que esse tratamento ulterior é do interesse do contribuinte e não houver razões para supor que o indivíduo não consentiria se tivesse conhecimento da outra finalidade; (iv) se a operação for necessária para desenvolver, rever ou alterar os procedimentos automatizados das autoridades fiscais; (v) se for preciso efetuar avaliações de impacto regulamentar; (vi) para o exercício dos poderes de supervisão, regulamentação das autoridades fiscais, ainda que para efeitos de treinamento ou teste, desde que o titular dos dados em causa não tenha interesses superiores que mereçam proteção.

Segundo a norma, no caso dos itens “iv” e “v”, a utilização posterior desses dados, no bojo dos procedimentos das autoridades fiscais, se justificaria quando fosse necessária uma coleta de dados inalterados ou quando o processo de anonimização ou de pseudonimização fosse impossível ou exigisse um esforço desproporcionado. Além disso, a lei também prevê que, nos casos em que se aplica o item “iv”, os dados devem ser apagados no prazo de um ano após a conclusão das medidas previstas nesse tópico.

Na situação prevista no item “i”, é “suficiente para tanto a relação funcional entre o tratamento posterior e o novo processo”. Em que pese a necessidade de observância do princípio da proporcionalidade, bem como, nos termos do art. 5º do RGPD, dos princípios da minimização dos dados e da limitação de conservação, a autoridade competente para o primeiro tratamento dos dados “goza de certo espaço de prognose ao decidir sobre o tratamento posterior de dados”, o que “alcança, sobretudo e fundamentalmente, a troca de informações e a assistência mútua entre os órgãos fiscais (§ 194, par. 3, AO)”²⁵⁹.

Importante pontuar, ainda, a previsão do § 29b, par. 2, primeira parte, que menciona a regra de exceção ao tratamento de dados sensíveis insculpida no art. 9º, par. 2, alínea g, do RGPD. Segundo esse dispositivo, a ressalva é válida caso haja a necessidade de tratamento por conta de relevante interesse público, com base “no direito da União ou de um Estado-Membro, que deve ser proporcional ao objetivo visado, respeitar a essência do direito à proteção dos dados pessoais e prever medidas adequadas e específicas que salvaguardem os direitos fundamentais e os interesses do titular dos dados”²⁶⁰. Exige-se, assim, que o interesse da autoridade fiscal se sobreponha ao interesse do particular titular dos dados. Ademais, a parte

²⁵⁹ SEER, 2020, p. 33.

²⁶⁰ UNIÃO EUROPEIA, ref. 20.

final do § 29b, par. 2, impõe procedimentos especiais voltados à salvaguarda dos interesses subjetivos do indivíduo, que devem ser observados pelo Fisco.

Já o par. 2 do § 29c da AO autoriza o tratamento posterior de dados sensíveis. Essa previsão pode operar em favor do contribuinte, no caso, por exemplo, do exame de dados para o cálculo de deduções tributárias a seu favor (v.g., análise de despesas médicas).

No que concerne ao dever de informar o titular de dados, os §§ 32a e 32b cuidam dessa obrigação para a coleta direta e junto a terceiros, respectivamente. O § 32a, par. 1, n. 1, dispensa a obrigação de comunicar caso a informação possa colocar em risco o desempenho de atividades da Administração Tributária ou quando o interesse público se sobrepuser ao interesse do titular dos dados. O § 32a, par. 2, por sua vez, traz exemplos em que o legislador presume fundamentos de perigo e, assim, afasta o dever de informar. Veja-se a redação desses dispositivos²⁶¹:

(1) Além da exceção especificada no Artigo 13(4) do Regulamento (UE) 2016/679, a obrigação das autoridades fiscais de informar o titular dos dados em conformidade com o Artigo 13(3) do Regulamento (UE) 2016/679 não se aplica se a prestação de informações sobre o tratamento ou divulgação posterior pretendidos:

1. prejudicar o desempenho efetivo das funções, conforme descrito no Artigo 23(1)(d) a (h), do Regulamento (UE) 2016/679, que são de competência das autoridades fiscais e o interesse das autoridades fiscais em não fornecer as informações prevalecer sobre os interesses do titular dos dados,
2. colocar em risco a segurança ou a ordem pública ou for prejudicial ao bem-estar da Federação ou de um país e o interesse das autoridades fiscais em não fornecer as informações prevalece sobre os interesses do titular dos dados,
3. impedir a capacidade da Federação, de um Estado ou de um município – como representante legal de uma autoridade tributária – de estabelecer, exercer ou defender reivindicações de direito civil ou de se defender contra reivindicações de direito civil na acepção do Artigo 23(1)(j) do Regulamento (UE) 2016/679 e a autoridade tributária não for obrigada pelo direito civil a fornecer informações, ou
4. colocar em risco a divulgação confidencial de dados protegidos a entidades públicas.

(2) O desempenho efetivo das funções, conforme descrito no Artigo 23(1)(d) a (h), do Regulamento (UE) 2016/679, que estão sob a jurisdição das autoridades fiscais será considerado prejudicado, em particular, se a prestação de informações:

1. puder permitir que o titular dos dados ou terceiros:
 - a) ocultar fatos ou circunstâncias que sejam relevantes para fins fiscais,
 - b) encobrir pistas que sejam relevantes para fins fiscais,
 - c) adequar a forma e a extensão de sua cooperação com as autoridades fiscais ao nível de informações em poder das autoridades fiscais, ou

²⁶¹ ALEMANHA, ref. 258.

2. possibilitar fazer inferências sobre o projeto de sistemas automatizados de gerenciamento de riscos ou medidas planejadas de controle/fiscalização e, assim, prejudicar seriamente a detecção de fatos ou circunstâncias relevantes para fins fiscais (tradução nossa).

Os parágrafos seguintes do § 32a tratam da necessidade de o Fisco tomar as medidas adequadas para proteger os interesses legítimos do titular de dados, caso seja afastado o dever de informar (par. 3), bem como da obrigação da autoridade de fornecer informações, se o eventual motivo de natureza temporária para a não comunicação cessar, “levando em conta as circunstâncias específicas do caso, dentro de um período razoável, mas não superior a duas semanas” (par. 4). O § 32b, por seu turno, estende os fundamentos para o afastamento da obrigação à coleta de dados pessoais realizada junto a terceiros.

À luz do art. 51, par. 1, do RGPD²⁶², o legislador alemão determinou que a autoridade federal de proteção de dados e liberdade de expressão, *Bundesbeauftragte für den Datenschutz und die Informationsfreiheit* (BfDI), é o órgão de controle em matéria de tratamento de dados no âmbito da aplicação do Código Tributário alemão. Nos termos da Lei Federal de Proteção de Dados germânica (*Bundesdatenschutzgesetz – BDSG*), o BfDI possui poderes de supervisão das autoridades fiscais.

Por fim, o § 32i prevê – em linha com os arts. 78 e 79 do RGPD, que tratam do direito à ação judicial contra a autoridade de controle, o responsável pelo tratamento ou o subcontratante –, o direito à tutela jurisdicional do titular de dados. Assim, atribui-se à Justiça Fiscal a competência para apreciar as causas contra o BfDI ou contra a autoridade fiscal, o que possibilita o acesso do contribuinte ao Judiciário em casos de inércia da autoridade supervisora ou de recusa injustificada de fornecimento de dados pelo Fisco.

As inovações normativas acima delineadas refletem o esforço do legislador em buscar uma compatibilização com o novo ambiente digital, mas, ao mesmo tempo, por conta da profundidade, podem exigir um exame de fatos e prognoses legislativos.

²⁶² “Artigo 51.º

Autoridade de controlo

1. Os Estados-Membros estabelecem que cabe a uma ou mais autoridades públicas independentes a responsabilidade pela fiscalização da aplicação do presente regulamento, a fim de defender os direitos e liberdades fundamentais das pessoas singulares relativamente ao tratamento e facilitar a livre circulação desses dados na União («autoridade de controlo»). UNIÃO EUROPEIA, ref. 20.

Na doutrina do professor Gilmar Mendes, a aferição dos fatos e prognoses consiste, no campo da jurisdição constitucional, em um “controle de resultado (*Ergebniskontrolle*) e não um controle do processo (*Verfahrenskontrolle*)”. Dessa maneira, não se investiga a forma a qual o parlamento analisou os fatos legislativos, mas “o *que*, efetivamente, ele constatou”²⁶³. Se a verificação de fatos realizada pelo legislador em relação a alguma regra restritiva for incorreta ou insuficiente, a norma pode incorrer em violações a bens jurídicos fundamentais.

Com a finalidade de atrair a legislação tributária alemã para o escopo da proteção de dados, buscou-se, quase que de forma exaustiva, dispor sobre as possibilidades de tratamento de dados pelo Fisco alemão. Ocorre que algumas situações precisam ser melhor investigadas, a exemplo das exceções à regra de prestação de informações sobre o tratamento ou divulgação posterior de dados.

Como visto, o § 32a afasta o dever de informação caso haja a possibilidade de comprometimento das atividades do órgão tributário e quando o interesse da autoridade se sobrepuser ao do titular dos dados. O dispositivo também elenca situações em que, presumidamente, o dever de comunicar possa gerar algum risco, como a possibilidade de o titular ocultar informações ou provas relevantes para fins fiscais ou de se fazer deduções sobre o sistema de fiscalização que poderiam prejudicar o controle.

Essas diretrizes geraram um nítido elastecimento das possibilidades de tratamento de dados sem a ciência do titular, que, em certa medida, podem dissentir da realidade. Com a utilização ostensiva de dados para toda e qualquer operação e em face da vagueza dos preceitos aplicados pelo legislador alemão, o dever de informação pode acabar sendo elidido pelo ideal de eficiência e de fiscalização.

Afinal, consoante a leitura das hipóteses elencadas na mencionada norma, há um amplo leque de situações em que é possível presumir um risco de comprometimento da atividade fiscalizadora. À vista disso, as fundamentações acerca da possibilidade de perigo, para fins de dispensa de prestação de informações, devem ser calcadas em situações de risco concreto e sempre com a exigência de justificativa formal. Do contrário, a norma validaria uma presunção absoluta contra o titular, que permitiria o controle desmedido de dados pessoais sem

²⁶³ MENDES, Gilmar Ferreira. Controle de Constitucionalidade: Hermenêutica Constitucional e Revisão de Fatos e Prognoses Legislativos pelo Órgão Judicial. **Revista de Direito Constitucional e Internacional**, v. 8, n. 31, p. 90-108, abr./jun. 2000.

a mínima observância do dever de comunicação.

3.5.2 A interpretação do BVerfG quanto à limitação do sigilo fiscal

O direito à informação sobre o tratamento de dados pode, invariavelmente, comportar balizas naturais no âmbito fiscal, como exemplifica o julgamento paradigmático do 1 BvR 2388/03²⁶⁴, em que o BVerfG definiu alguns limites às reivindicações sobre coleta de dados. Naquele julgado, o requerente desejava obter informações, junto ao centro de informações tributárias estrangeiras do órgão fiscal federal central (*Bundeszentralamt für Steuern – BZSt*), sobre os dados guardados a seu respeito. Isso porque a autoridade fiscal alemã possuía algumas extensas pastas de arquivos armazenadas, nas quais seu nome estaria ligado direta ou indiretamente a operações com empresas estrangeiras.

O contribuinte alegava que, com base no § 19 da Lei Federal de Proteção de Dados (*Bundesdatenschutzgesetz*)²⁶⁵, possuiria o direito de acesso a essas informações. A autoridade se recusou a fornecê-las, sob o argumento de que, com base nessa mesma norma, os dados não devem ser disponibilizados se isso for prejudicial ao adequado desempenho das funções do órgão competente.

A Corte Constitucional alemã concluiu que, apesar de o interesse do reclamante em obter informações sobre as medidas oficiais relacionadas aos dados que lhe dizem respeito ser, em tese, protegido por seu direito constitucional à autodeterminação informativa, essa tutela não abrangeria a reivindicação então pretendida.

Considerou o BVerfG que, na medida em que houver interesses conflitantes entre a confidencialidade do Estado ou de terceiros e o fornecimento de informações, o legislador deve desenvolver exceções apropriadas que levem em conta esses embates. Nessa linha, destacou-se que o § 19 da *Bundesdatenschutzgesetz* fez essa ponderação ao impedir que a reivindicação de informações, pelo titular dos dados, esbarre no desempenho adequado das funções

²⁶⁴ ALEMANHA. Bundesverfassungsgericht. **1 BvR 2388/03**. BverfGE, n. 120, 2008. Disponível em: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2008/03/rs20080310_1_bvr238803.htm. Acesso em: 20 maio 2023.

²⁶⁵ O dispositivo regulamenta a competência para julgamento de representações atinentes ao capítulo VII do RGPD (disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679>; acesso em: 20 maio 2023). O referido capítulo trata da cooperação entre as autoridades. Disponível em: https://www.gesetze-im-internet.de/bdsg_2018/BDSG.pdf. Acesso em: 20 maio 2023.

estatais.

Assim, ao se aplicar a exceção estabelecida no § 19 da Lei Federal, pondera-se o interesse constitucionalmente protegido do reclamante em obter informações com o interesse público conflitante no desempenho adequado das funções da autoridade fiscal.

A Corte destacou que, caso os dados fossem compartilhados com o titular, o objetivo da coleta daquelas informações seria frustrado: seriam reveladas ao contribuinte informações sobre quais operações a autoridade fiscal já teria ciência, de modo que o titular dos dados poderia ajustar sua conduta de acordo com o *status* do conhecimento mantido pelo Fisco alemão. Em consequência, esses dados seriam em grande parte destituídos de valor após essa comunicação.

Contudo, restou expressamente consignado, naquele julgado, que seria dissonante do texto constitucional opinião no sentido de o interesse do contribuinte ser comparativamente menos importante do que o objetivo de cobrança igualitária de tributos buscado por meio da manutenção do sigilo.

Nessa senda, pontuou-se que, como resultado dessa regra de exceção ao seu direito à autodeterminação informativa, deve-se sempre assegurar que a coleta e o armazenamento de dados estejam corretos, de modo que as informações sejam utilizadas apenas para os fins fiscais especificamente designados. Assim, asseverou-se ser imperativo garantir, a esse respeito, que o titular não sofra desvantagens devido a esse impedimento legal de acesso.

3.5.3 As ponderações acerca da publicização de dados de contribuintes húngaros

A Câmara da Quarta Seção do Tribunal Europeu dos Direitos Humanos (TEDH) enfrentou uma relevante controvérsia relacionada à contraposição entre o direito à privacidade e o dever de publicidade no contexto de divulgação de informações pela autoridade fiscal²⁶⁶.

Em janeiro de 2016, o órgão tributário húngaro divulgou, em seu site oficial, com base na legislação local vigente, uma lista de “grandes sonegadores de impostos”, que indicava os cidadãos inadimplentes devedores de mais de 10 milhões de florins húngaros (cerca de 136 mil reais) no trimestre anterior. As

²⁶⁶ TEDH. **Case of L.B. v. Hungary**, app. nº 36345/16. Fourth Section, j. 12/1/2021. Disponível em: <https://hudoc.echr.coe.int/eng?i=001-207132>. Acesso em: 20 jun. 2023.

informações publicadas nessa listagem incluíam o nome, o endereço, o número de identificação e o valor da dívida tributária.

Além disso, segundo relatado na decisão, foi lançado um “mapa nacional de inadimplentes fiscais”, no qual o endereço do devedor ficava “indicado com um ponto vermelho e, se uma pessoa clicasse no ponto, as informações pessoais do requerente (nome e endereço residencial) apareciam, portanto, os dados estavam disponíveis para todos os leitores” (tradução nossa)²⁶⁷.

O requerente, Sr. L.B., cidadão húngaro residente em Budapeste, apresentou uma espécie de reclamação ao TEDH, pela qual alegava violação ao art. 8º da Convenção Europeia dos Direitos Humanos (CEDH), que trata sobre o “direito ao respeito pela vida privada e familiar”²⁶⁸. Argumentava-se, nesse sentido, que a medida prevista na legislação húngara objetivava, unicamente, constranger publicamente o cidadão e não asseguraria necessariamente uma maior eficiência na arrecadação de tributos. Já a autoridade fiscal húngara afirmava que o objetivo de sua regulamentação era garantir o bem-estar econômico do país, bem como proteger os direitos de terceiros, isto é, os potenciais parceiros comerciais do requerente.

Como registrou o TEDH, o contribuinte não negou que a atuação do Poder Público húngaro encontrava respaldo em sua legislação local. O procedimento, como mencionado inúmeras vezes na decisão, era previsto nas normas sobre a Administração Tributária daquele país.

Assim, não se discutia a legalidade da medida, mas, sim, sua legitimidade com base na CEDH. Nessa perspectiva, ao analisar a política implementada à luz do princípio da necessidade, o TEDH avaliou se a autoridade fiscal húngara havia realizado uma justa ponderação entre o direito do requerente à privacidade e o

²⁶⁷ No original: “On 16 February 2016 an online media outlet produced an interactive map called ‘the national map of tax defaulters’. The applicant’s home address, along with the addresses of other tax defaulters, was indicated with a red dot, and if a person clicked on the dot the applicant’s personal information (name and home address) appeared, thus the data was available to all readers”. TEDH, ref. 266.

²⁶⁸ “ARTIGO 8º

Direito ao respeito pela vida privada e familiar

1. Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência.

2. Não pode haver ingerência da autoridade pública no exercício deste direito senão quando esta ingerência estiver prevista na lei e constituir uma providência que, numa sociedade democrática, seja necessária para a segurança nacional, para a segurança pública, para o bem-estar económico do país, a defesa da ordem e a prevenção das infracções penais, a protecção da saúde ou da moral, ou a protecção dos direitos e das liberdades de terceiros.” TEDH. **Convenção Europeia dos Direitos Humanos**. Roma, 1950.

interesse público geral.

Por maioria, a Câmara do Tribunal pontuou que “não acha irracional que o Estado considere necessário proteger seu interesse econômico geral na arrecadação de receita pública por meio de escrutínio público com o objetivo de dissuadir as pessoas de não cumprirem suas obrigações fiscais” (tradução nossa)²⁶⁹. Nessa toada, prevaleceu o entendimento de que a regra fomentava a política tributária húngara e protegia o interesse econômico geral ao informar previamente à sociedade que determinado cidadão não cumpria suas obrigações tributárias.

Dessa maneira, a escolha política de tornar públicos os dados pessoais dos inadimplentes se alinhava à legítima finalidade da medida, eis que essa divulgação funcionaria como uma ferramenta para desincentivar o inadimplemento, bem assim para proteger os interesses comerciais de terceiros.

Além disso, o órgão julgador justificou a proporcionalidade da regra, porque a publicização de dados era autorizada apenas para as situações específicas da lei, isto é, se o contribuinte fosse devedor de uma monta considerável de tributos por mais de 180 dias. Nesse ponto, verifica-se que o legislador adotou uma distinção entre contribuintes com base em critérios que julgou relevantes para justificar a prevalência do interesse público sobre os direitos de personalidade desses “grandes sonegadores”. Para a Câmara, “a medida foi circunscrita para tratar do risco de distorção do sistema tributário, e o legislador limitou qualquer efeito negativo dessa publicação àqueles cuja conduta era mais prejudicial à receita” (tradução nossa)²⁷⁰.

Contudo, é ressaltado na decisão que, apesar de dados como o nome e o endereço residencial não tratarem da intimidade do contribuinte e poderem ser facilmente extraídos por outros meios, como listas telefônicas, a divulgação dessas informações no contexto examinado poderia trazer severas repercussões na vida privada do requerente. Mas, nas circunstâncias daquele julgamento, o órgão julgador considerou que a lista de inadimplentes seria inútil caso não permitisse a identificação dos contribuintes em questão, o que não seria possível apenas com a disponibilização do nome e do sobrenome. Por conseguinte, na visão do órgão, a

²⁶⁹ No original: “*The Court does not find it unreasonable that the State considers it necessary to protect its general economic interest in collecting public revenue by means of public scrutiny aimed at deterring persons from defaulting on their tax obligations*”. TEDH, ref. 266.

²⁷⁰ No original: “*The Court therefore accepts that the measure was circumscribed to address the risk of distortion of the tax system, and the legislature limited any negative effect of such publication to those whose conduct was the most detrimental to revenue [...]*”. TEDH, ref. 266.

publicação desses dados pessoais seria necessária para alcançar o objetivo de facilitar o “escrutínio público da evasão fiscal”.

Ademais, pontuou-se que uma lista restrita aos nomes dos contribuintes conteria informações imprecisas e poderia acarretar consequências negativas para pessoas com o mesmo nome do devedor.

Em seguida, concluiu a Câmara do TEDH²⁷¹:

[...] Por outro lado, o Tribunal encontra força no argumento do Governo de que o acesso público generalizado aos dados em questão era necessário para a eficácia do esquema (ver parágrafo 41 acima). Embora reconhecendo a importância dos direitos de uma pessoa que tenha sido objeto de conteúdo disponível na Internet, esses direitos também devem ser equilibrados com o direito do público de ser informado (ver *M.L. e W.W. v. Germany*, nos. 60798/10 e 65599/10, § 104, 28 de junho de 2018). No presente caso, a finalidade e o principal efeito da publicação foram informar o público, e a principal razão para disponibilizar esses dados na Internet foi tornar as informações facilmente disponíveis e acessíveis aos interessados, independentemente de seu local de residência (tradução nossa).

Portanto, o interesse público, considerando todo o cenário de implementação da política húngara, prevaleceu sobre os direitos de personalidade do requerente. Também corroborou essa conclusão o argumento de que o alcance da lista não seria tão amplo, já que o documento estava escrito em húngaro, língua pouco usual no restante do mundo, e era publicado apenas no site oficial da autoridade fiscal local, o que asseguraria que tais informações fossem distribuídas de uma maneira “razoavelmente calculada para alcançar aqueles com um interesse particular nelas, enquanto evitava a divulgação para aqueles que não tinham tal interesse”.

A Câmara também afirmou que o site da autoridade tributária não oferecia ao público qualquer ferramenta que permitisse algum tipo de ataque ao requerente, a exemplo de mecanismos de interação entre usuários do portal. Por fim, é ressaltado na decisão que o Sr. L.B. não havia apontado nenhuma prova que indicasse quaisquer repercussões concretas em sua vida privada decorrentes da publicização de seus dados pessoais. Dessa forma, a divulgação dos dados pessoais do

²⁷¹ No original: “On the other hand, the Court finds force in the Government’s argument that widespread public access to the data concerned was necessary for the efficacy of the scheme (see paragraph 41 above). While recognising the importance of the rights of a person who has been the subject of content available on the Internet, these rights must also be balanced against the public’s right to be informed (see *M.L. and W.W. v. Germany*, nos. 60798/10 and 65599/10, § 104, 28 June 2018). In the present case, the purpose and the principal effect of publication were to inform the public, and the main reason for making such data available on the Internet was to make the information easily available and accessible to those concerned, irrespective of their place of residence”. TEDH, ref. 266.

contribuinte não representava, na visão da maioria dos juízes daquela Câmara, um ônus substancialmente maior para sua vida privada do que o necessário para promover o interesse legítimo do Estado. Assim, não haveria, no caso, violação ao art. 8º da CEDH.

Todavia, é importante destacar que a conclusão em relação à ausência de violação ao referido dispositivo não foi unânime. Dois dos sete votos – proferidos pelos juízes Ravarani e Schukking – concluíam que a publicação do endereço residencial e a divulgação dos dados na internet seriam desnecessárias para o cumprimento do objetivo da lei. Demais disso, a decisão foi criticada pelo fato de haver ignorado, no exame da violação ao direito à privacidade, a possibilidade de republicação dos dados pessoais por terceiros, tendo apenas se limitado a afirmar que o alcance da divulgação no site oficial da autoridade fiscal estaria restrito aos poucos interessados²⁷².

No que tange à disponibilização do endereço, os votos dissidentes assinalavam que haveria outros meios suficientes para que os interessados pudessem identificar aqueles com quem valeria a pena fazer negócios. Aliás, se esse fosse o intuito, bastaria que fosse possível preencher o nome e o número de identificação para que a plataforma oficial indicasse se o indivíduo possuiria, ou não, alguma dívida tributária.

Também foi apontada a ausência de salvaguardas adicionais em relação à publicação de dados pessoais na rede mundial de computadores. A divulgação de informações na internet, como aponta o voto divergente, tem um “imenso efeito multiplicador”, o que possibilita, por consequência, que muitos “não interessados” acessem os dados que, na visão da maioria dos juízes, estariam limitados aos potenciais parceiros comerciais dos inadimplentes húngaros. A grande repercussão desse caso no TEDH, por si só, já afasta o argumento do alcance restrito da ferramenta.

Com essa ampla disseminação, surgem riscos significativos aos contribuintes que figuram no “mapa nacional de inadimplentes fiscais”, os quais podem ter seus dados pessoais integrados a outras bases e, assim, utilizados para outras

²⁷² Cf., a propósito, KEUNEN, Liesa. **The right to privacy used as a modern pillory in L.B. v. Hungary.** Strasbourg Observers, 2021. Disponível em: <https://strasbourgobservers.com/2021/03/01/the-right-to-privacy-used-as-a-modern-pillory-in-l-b-v-hungary/>. Acesso em: 20 jun. 2023; PURPURA, Andrea. Case Law Note: Protection of Taxpayers' Personal Data and National Tax Interest: A Misstep by the European Court of Human Rights? **Intertax**, v. 49, n. 12, p. 1044-1055, 2021.

finalidades, como, e.g., as atividades comerciais de seguradoras e bancos²⁷³.

Por fim, considerando a potencial repercussão da republicação dos dados, é irrelevante que as informações sejam disponibilizadas por tempo limitado. Como apontado no voto divergente, “não há ‘direito ao esquecimento’ quando alguém é pego na ‘teia da internet’”. Da mesma forma, não seria tarefa simples demonstrar as repercussões concretas na vida privada do contribuinte. Afinal, segundo a manifestação dissidente, essa prova é “extremamente difícil de ser apresentada e geralmente permanece na esfera moral, onde o impacto concreto de tal medida é simplesmente impossível de ser medido objetivamente” (tradução nossa)²⁷⁴.

Em março de 2023, o caso voltou a ser apreciado na Corte, desta feita em sede de recurso perante a *Grand Chamber* do TEDH²⁷⁵. Por quinze votos a dois, concluiu-se que houve, de fato, violação ao art. 8º da CEDH.

Embora tenha aceitado que a intenção do legislador era aprimorar a adimplência fiscal, o órgão superior do Tribunal considerou que o Estado não demonstrou que teria buscado encontrar um equilíbrio justo entre os interesses concorrentes relevantes, com vista a garantir a proporcionalidade da interferência. Nesse ponto, destacou o órgão julgador²⁷⁶:

133. Em particular, não parece que o Parlamento avaliou até que ponto a publicação de todos os elementos da lista da seção 55(5), mais notavelmente o endereço residencial do devedor de impostos, era necessária para alcançar um efeito dissuasivo, como sugerido pelo

²⁷³ KEUNEN, ref. 272.

²⁷⁴ No original: “*It appears sanctimonious to state that the applicant had not demonstrated concrete repercussions on his private life. Such evidence is extremely difficult to adduce and it usually remains in the moral sphere, where the concrete impact of such a measure is simply impossible to measure objectively*”. TEDH, ref. 266.

²⁷⁵ TEDH. **Case of L.B. v. Hungary, app. nº 36345/16**. Grand Chamber, j. 9/3/2023. Disponível em: <https://hudoc.echr.coe.int/fre#%7B%22itemid%22:%5B%22001-223675%22%7D>. Acesso em: 20 jun. 2023.

²⁷⁶ No original: “133. *In particular, it does not emerge that Parliament assessed to what extent publication of all the elements of the section 55(5) list, most notably the tax debtor’s home address, was necessary to achieve a deterrent effect, as suggested by the Government, in addition to that of tax defaulters identified on a separate list pursuant to section 55(3) of the 2003 Tax Administration Act [...] 134. The Court further observes that while the explanatory report to the 2003 Tax Administration Act referred to taxpayers’ right to privacy as justification for strict rules on confidentiality (see paragraph 12 above), there is no evidence that consideration was given to the impact of the section 55(5) publication scheme on the right to privacy, and in particular the risk of misuse of the tax debtor’s home address by other members of the public (see paragraph 14 above). 135. Nor does it appear that consideration was given to the potential reach of the medium used for the dissemination of the information in question, namely the fact that the publication of personal data on the Tax Authority’s website implied that irrespective of the motives in obtaining access to the information anyone, worldwide, who had access to the Internet also had unrestricted access to information about the name as well as the home address of each tax debtor on the list, with the risk of republication as a natural, probable and foreseeable consequence of the original publication*”. TEDH, ref. 275.

Governo, além daquele dos inadimplentes de impostos identificados em uma lista separada de acordo com a seção 55(3) da Lei de Administração Tributária de 2003 [...]

134. A Corte observa ainda que, embora o relatório explicativo da Lei de Administração Tributária de 2003 tenha se referido ao direito dos contribuintes à privacidade como justificativa para regras rígidas de confidencialidade (ver parágrafo 12 acima), não há evidência de que tenha sido considerado o impacto do esquema de publicação da seção 55(5) sobre o direito à privacidade e, em particular, o risco de uso indevido do endereço residencial do devedor de impostos por outros membros do público (ver parágrafo 14 acima).

135. Tampouco parece ter sido considerado o alcance potencial do meio utilizado para a disseminação das informações em questão, ou seja, o fato de que a publicação de dados pessoais no site da Autoridade Tributária implicava que, independentemente dos motivos para obter acesso às informações, qualquer pessoa, em todo o mundo, que tivesse acesso à Internet também teria acesso irrestrito às informações sobre o nome e o endereço residencial de cada devedor tributário da lista, com o risco de republicação como consequência natural, provável e previsível da publicação original (tradução nossa).

Portanto, a exegese da Câmara Superior pautou-se nas falhas incorridas nas prognoses do legislador quanto aos interesses conflitantes em jogo. Em outras palavras, ponderou a maioria dos juízes que não houve um correto exame de proporcionalidade, de modo que, levando em consideração a salvaguarda do direito à privacidade e o princípio da minimização do uso de dados pessoais, medidas menos restritivas poderiam ter sido adotadas pelo Parlamento húngaro para as finalidades pretendidas.

3.5.4 O caso americano *Harper v. Rettig*

Recentemente, em movimento encabeçado por uma associação de defesa das liberdades individuais (*New Civil Liberties Alliance* – NCLA), nos Estados Unidos, foram firmadas orientações cruciais acerca da inafastabilidade da jurisdição para a salvaguarda da garantia da privacidade em face das regras que legitimam o poder-dever da Administração Tributária de fiscalizar e arrecadar.

No caso *James Harper v. Charles P. Rettig, in His Official Capacity as IRS Comm'r, IRS & John Doe IRS Agents 1-10*²⁷⁷, discutia-se se o contribuinte James Harper poderia postular contra a agência federal tributária dos Estados Unidos – *Internal Revenue Service* (IRS) –, perante o Poder Judiciário federal, em razão de o

²⁷⁷ ESTADOS UNIDOS. United States Court of Appeals For the First Circuit. **James Harper v. Charles P. Rettig, in His Official Capacity as IRS Comm'r, IRS & John Doe IRS Agents 1-10**. Case 21-1316 (2022). Boston, 2022.

órgão haver coletado, em bases de terceiros, suas informações privadas sobre transações com moedas virtuais, com a finalidade de investigar a ocorrência de eventuais obrigações tributárias.

Na ocasião, o cidadão apontava violação às suas garantias constitucionais, eis que as informações foram extraídas de seus registros financeiros pessoais armazenados em uma casa de câmbio digital, ou seja, sem qualquer autorização ou ciência, seus dados disponibilizados a terceiros foram coletados pela autoridade. Assim, a defesa de Harper argumentava que o contribuinte teria direito de postular em juízo contra o órgão fiscal, a fim de que houvesse o devido processo de responsabilização pelos atos abusivos de coleta de dados.

O IRS, por seu turno, negava esse direito de postulação, sob o argumento de que, caso fosse permitido que os cidadãos se opusessem às operações de coleta de dados pessoais, haveria um prejuízo à atividade fiscalizadora das autoridades tributárias. Em linha com essa afirmação, o Tribunal Distrital de New Hampshire (*U.S. District Court for the District of New Hampshire*), em 2021, concluiu pela impossibilidade de julgamento da causa, com base na *Anti-Injunction Act of the Internal Revenue Code* (26 U.S.C. § 7421), que vedaria o ajuizamento de ação com o objetivo de impedir a autuação ou a cobrança de qualquer tributo.

A questão relacionada ao acesso à jurisdição para os pleitos contra a coleta de dados pelo IRS era matéria controvertida no direito americano, ante as possíveis leituras da referida norma. No entanto, em agosto de 2022, o colegiado de três juízes da Corte de Apelações americana do Primeiro Circuito (*U.S. Court of Appeals for the First Circuit*), por unanimidade de votos, reformando decisão do Tribunal Distrital, concluiu que a recolha de informações do apelante, pela IRS, seria indevida e, a partir de um juízo de sobreposição das garantias constitucionais aos deveres arrecadatários do Fisco, o titular dos dados teria o direito de postular em juízo.

Nos termos do paradigmático voto condutor do Juiz Kermit Lipez, ponderou-se que a Suprema Corte americana, em julgamento recente²⁷⁸, haveria esclarecido que a regra da *Anti-Injunction Act* não seria aplicável inalteradamente a toda e qualquer atividade que possa melhorar a capacidade de fiscalização e cobrança de tributos – como as ações de coleta de dados –, mas apenas aos próprios atos de liquidação e cobrança do débito fiscal.

²⁷⁸ Cf. ESTADOS UNIDOS. **Supreme Court of the United States. CIC Services, LLC v. Internal Revenue Service**, 593 U.S. 19-930 (2021). Washington, 2021.

Destacou o magistrado que a referida lei “não impediria uma ação judicial que questionasse exigências comuns de declaração, mesmo que essas exigências ‘facilitem [a] cobrança de impostos’ ao identificar os contribuintes que devem impostos” (tradução nossa). Em seguida, ressaltou que, contrariamente ao que sugeria o IRS, o pleito do contribuinte não esbarraria no óbice da *Anti-Injunction Act*, uma vez que o procedimento não seria contra o tributo em si, mas, sim, contra os métodos – ou os meios – utilizados pelo Fisco americano para a obtenção de informações²⁷⁹.

Com esses argumentos, a sentença de indeferimento foi anulada e o processo foi remetido ao Tribunal Distrital de New Hampshire para um novo julgamento, agora orientado por esses contornos concernentes ao cabimento da medida judicial.

A distinção feita nesse julgamento, apesar de aparentar, em uma primeira análise, ser sutil, levanta relevantes considerações sobre os limites impostos à atividade fiscalizadora. Busca-se, com essa interpretação, conter os excessos por parte das autoridades, de modo a impedir que a finalidade arrecadatória seja uma carta branca para todo e qualquer ato de coleta de dados dos contribuintes.

3.6 Breves reflexões sobre a Reforma do Sistema Tributário brasileiro

Por derradeiro, fazendo algumas considerações sobre o contexto atual, é importante destacar que os debates levantados nesta pesquisa precisam caminhar em harmonia com as proposições apresentadas na iminente Reforma do Sistema Tributário brasileiro.

Entre as propostas que tramitam no Parlamento brasileiro, a PEC nº 45/2019²⁸⁰ – que visa instituir o Imposto sobre Bens e Serviços (IBS), de competência dos Estados, do Distrito Federal e dos Municípios – é a que se encontra em estágio mais avançado. A medida prevê a implementação de um

²⁷⁹ No original: “Noting that ‘[i]nformation gathering’ ... is ‘a phase of tax administration procedure that occurs before assessment [or] collection,’ the Court explained that the *Anti-Injunction Act* would not bar a lawsuit challenging ordinary reporting requirements, even if those requirements ‘facilitate [the] collection of taxes’ by identifying taxpayers who owe tax, because reporting requirements are part of the information-gathering phase of tax administration.” ESTADOS UNIDOS, ref. 277.

²⁸⁰ BRASIL. Câmara dos Deputados. **Proposta de Emenda à Constituição nº 45, de 2019**. Altera o Sistema Tributário Nacional e dá outras providências. Brasília, DF, [2019]. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2196833>. Acesso em: 23 jun. 2023.

Imposto sobre Valor Agregado (IVA), que será devido a diversos Entes Federativos e incidirá sobre operações com bens materiais ou imateriais, inclusive direitos, ou com serviços.

Dessa forma, o constituinte derivado buscará criar um tributo que abarque as operações com produtos intangíveis, o que engloba os modelos de negócios do ciberespaço. Trata-se de medida que visa combater o fenômeno da erosão da base tributária, o qual decorre, em grande parte, da crescente tendência de digitalização da economia. Ao mesmo tempo, intenta-se, com a instituição de um IVA, propiciar a criação de um sistema menos oneroso e mais justo, voltado para o combate ao efeito cascata na tributação.

Será formado, nesse cenário, o Conselho Federativo do Imposto sobre Bens e Serviços, entidade pública sob regime especial, com independência técnica, administrativa, orçamentária e financeira, que terá as seguintes atribuições: edição de normas infralegais sobre temas relacionados ao IBS, uniformização da interpretação e da aplicação da legislação do imposto, recolhimento desse tributo e distribuição do produto da arrecadação entre Estados, Distrito Federal e Municípios, resolução de questões suscitadas no âmbito do contencioso administrativo tributário entre o sujeito passivo e a Administração Tributária etc.

Considerando que o órgão acumulará as competências dos Estados e dos Municípios, bem assim que terá a incumbência de dirimir os conflitos decorrentes do contencioso administrativo fiscal e de monitorar a cobrança do tributo, é possível inferir que a entidade possuirá amplos poderes e uma extensa base de dados para não só tributar as operações digitais, mas também fiscalizar os sujeitos passivos.

Tem-se, portanto, relevante questão a ser pensada no bojo das discussões sobre o uso de dados dos contribuintes. Um “Super Fisco”, com diversas competências procedimentais e com atribuição para tributar operações com bens imateriais, precisaria ter sua atividade bem delimitada. Nessa perspectiva, é imprescindível que a lei complementar que regulamentará a sua atuação, ao ponderar esses aspectos, leve em consideração os parâmetros anteriormente abordados.

CONSIDERAÇÕES FINAIS

“Mas eu lhe garanto, Winston, a realidade não é externa. A realidade existe na mente humana e em nenhum outro lugar.”

(George Orwell)²⁸¹

Assim como na narrativa do célebre autor George Orwell, em que o “*Big Brother*” criava uma realidade própria para justificar suas regras de vigilância ostensiva, as normas de governança de dados, a pretexto de assegurarem o poder de polícia, sustentam-se por um ideário fiscalizatório expansivo. Essa analogia é ainda mais evidente nas operações fiscais, em que, com base nos objetivos da Administração Tributária, busca-se otimizar o controle das operações dos contribuintes no ambiente digital para perseguir o objetivo arrecadatório da atividade estatal plenamente vinculada.

Com isso, nesta pesquisa, foram analisadas as zonas de intersecção entre as operações de tratamento de dados pela autoridade tributária brasileira e as diretrizes de salvaguarda da privacidade e da proteção de dados dos contribuintes. Dessa forma, com base na leitura do direito à intimidade a partir da concepção de um autocontrole das informações do titular, demonstrou-se que a garantia de sigilo fiscal não é um resguardo, por si só, suficiente para que se permita o livre fluxo dos dados dos usuários de serviços públicos.

Para tanto, examinou-se, inicialmente, as garantias constitucionais que devem reger as operações que envolvam a coleta e a transferência de dados pessoais de contribuintes. Nesse particular, viu-se que, em que pese se tratar de atividade há muito tempo desempenhada pelo Estado, ocorreram mudanças qualitativas e quantitativas nesse tratamento, haja vista a ascensão de novos métodos e tecnologias. Com a sofisticação da coleta e do cruzamento de dados, é cada vez mais “relevante e urgente o debate acerca das condições de contorno para o uso e

²⁸¹ ORWELL, George. **1984**. Tradução de Heloisa Jahn e Alexandre Hubner. São Paulo: Companhia das Letras, 2009.

tratamento de dados de cidadãos pelo Estado”²⁸².

Assim, discorreu-se, primeiramente, sobre o direito à privacidade. Orientando-se pela ideia de um direito à autodeterminação informativa, concluiu-se que, ainda que os dados apresentem baixo conteúdo informativo, pode haver intervenção na liberdade do indivíduo com as operações de coleta e transmissão de informações. Dessa forma, uma interpretação mais acertada da proteção da intimidade deve pautar-se na concepção dessa garantia como uma liberdade individual do contribuinte, definida como um poder de controlar, determinar e escolher as informações a seu respeito.

Essa visão é amparada pela referida interpretação de Daniel J. Solove da relação entre privacidade e segurança. Conforme aludido, a privacidade precisa ser considerada com base na sua multiplicidade de significados, afastando-se, assim o argumento do “nada a esconder”, que contempla apenas as hipóteses em que o cidadão pretende esconder “coisas ruins”.

No entanto, entre as várias interpretações dessa garantia constitucional, há também a noção da proteção do titular de dados nas relações com o Poder Público, que visa assegurar o conhecimento e a participação do indivíduo nesse processo. Nesse particular, Solove pondera que a problemática mais se assemelha à metáfora kafkiana do que ao conto de Orwell, considerando os obstáculos encontrados pelos cidadãos para a obtenção de informação ou a atuação no processo de utilização de seus dados.

Em seguida, com fundamento nas regras que amparam o exercício das competências legais dos órgãos fiscalizatórios, foram traçados os limites impostos às autoridades, os quais estão ancorados nas normas que tratam do sigilo fiscal. Nesse ponto, ao se abordar os atos normativos que tratam do dever de confidencialidade da Fazenda Pública, verificou-se que, em que pese a complexa regulamentação do acesso a informações protegidas pelo dever de sigilo, com a estipulação de limitações e penalidades, ainda há um extenso debate sobre a relativização da regra.

À luz dos julgados paradigmáticos do STF e em linha com as diretrizes internacionais, viu-se que, ante a situação de coexistência dos direitos à privacidade e à confidencialidade nas operações tributárias, é necessário que a transmissão de

²⁸² WIMMER, 2021, p. 271.

dados respeite a regra de manutenção do sigilo. É essencial, nesse sentido, fazer um juízo de ponderação dos preceitos insculpidos nos incisos X e XII do art. 5º da Constituição Federal, que não são absolutamente inafastáveis e, como visto, podem ser flexibilizados.

Essa discussão ganhou força nos últimos tempos, haja vista o valor que se passou a conferir aos dados. Hoje, as próprias informações pessoais podem ser valiosas, o que faz com que algumas das positivamente analisadas, pensadas para um contexto não mais condizente com a realidade da Era da Informação – notadamente a da última década –, possam conflitar com liberdades individuais.

Por exemplo, poder-se-ia exigir, a partir desse debate, um exame mais ponderado de dispositivos como o mencionado § 1º do art. 2º da Portaria RFB nº 2.344/2011, que excepciona da regra do sigilo as informações cadastrais do contribuinte e as relativas à sua regularidade fiscal.

Em seguida, foram estudados os atos normativos que regulamentam a troca de informações em matéria tributária e as regras vigentes sobre proteção de dados, notadamente aquelas relacionadas ao uso de informações pelo Poder Público. Por fim, foram feitas considerações sobre a aplicabilidade das normas sobre salvaguarda de dados pessoais às operações com o Fisco.

No intuito de melhor delinear os mecanismos utilizados pelo Fisco no tratamento de dados de contribuintes, foram explorados especialmente os decretos e atos infralegais atinentes à fiscalização na esfera federal.

Em primeiro lugar, constatou-se que o Decreto nº 10.046/2019, bem como a Portaria RFB nº 34/2021, que regulamentou o tema no âmbito fiscal, institucionalizaram uma extensa base de dados unificada, que possibilitaria um livre compartilhamento de informações de contribuintes entre os órgãos da Administração Pública federal. Isso levantou preocupações em relação ao potencial risco de violação às garantias de proteção de dados pessoais e de controle político dos titulares.

Apesar de a referida portaria haver buscado criar regras formais para a operacionalização do compartilhamento pela RFB, com requisitos bem definidos – a exemplo da identificação do órgão solicitante, da relação detalhada das informações requeridas, da descrição da forma e da periodicidade do recebimento dos dados, da demonstração da necessidade e da finalidade da operação, da indicação, da declaração de cumprimento dos requisitos de segurança previamente estipulados

etc. –, além da obrigação da correta utilização das informações recebidas, sob pena de interrupção da operação e de responsabilização, a norma ainda carece de disposições claras em relação à comunicação com o contribuinte, titular dos dados.

Sobre esse ponto, foi sinalizado que, embora haja expressa previsão, na LGPD, da possibilidade de o usuário solicitar “informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados” (art. 18, inciso VII), o titular apresenta dificuldade para exercer esse direito de controle informativo no âmbito das operações previstas na Portaria nº 34/2021, já que não é avisado sobre o uso de suas informações pessoais.

A mesma consideração vale para o aludido Decreto nº 10.209/2020, que buscou regulamentar a aplicação do art. 198 do CTN. A norma incorpora notável avanço em relação à proteção do contribuinte ao regulamentar o intercâmbio de informações sigilosas, que deve ser precedido pela instauração de procedimento administrativo próprio.

O diploma também dispõe sobre a restrição do uso dos dados às finalidades específicas de auditoria ou de inspeção de dados, de processos ou de controles operacionais da Administração Tributária e aduaneira, da gestão fiscal ou da análise de demonstrações financeiras da União, sendo vedadas as requisições de acesso a “dados genéricos, desproporcionais, imotivados ou desvinculados dos procedimentos de auditoria ou inspeção” e a publicização de informações protegidas por sigilo fiscal ou por sigilo profissional ou o repasse das informações a terceiros.

Como se pôde constatar, a despeito dessas previsões que conferem mais segurança aos procedimentos internos do Fisco federal, o decreto também não situa, dentro do debate, o dever de informação ao titular.

Em linha com essas preocupações, foi destrinchada a Portaria RFB nº 167/2022, que cria a possibilidade de o Serpro fornecer a terceiros o acesso a dados armazenados pela RFB. Destacou-se que o ato normativo possibilita a transmissão de inúmeros dados sigilosos custodiados pelo órgão fazendário, desde que o tratamento seja destinado ao fiel cumprimento de políticas públicas e em conformidade com a LGPD.

Mesmo com os esclarecimentos prestados pela RFB em relação à segurança dos procedimentos previstos na portaria, ainda remanescem dúvidas sobre a compatibilidade desses regramentos com a privacidade dos contribuintes. De fato, a norma não autoriza a “venda” de dados pessoais, como alguns mais alarmistas

chegaram a noticiar. No entanto, o ato normativo inaugura uma modalidade de compartilhamento, por meio de um contrato unilateral entre o Serpro e o terceiro solicitante, de várias informações tributárias consideravelmente sensíveis.

Dessa forma, essa solução tecnológica pode discrepar do figurino legal e constitucional da proteção à privacidade dos contribuintes. Isso porque os titulares dos dados sequer tomam conhecimento das razões e dos termos²⁸³ dos acordos firmados entre a RFB e os terceiros solicitantes. Igualmente gravoso é o fato de a norma não dispor de um rito de indicação de um encarregado ou dos agentes de tratamento, o que acaba distanciando essa portaria da aplicação das normas regulatórias da LGPD.

Por derradeiro, o Convênio ICMS nº 134/2016, apesar de versar sobre tributo estadual, traz uma norma de observância nacional que também gera inquietações. O acordo, ao disciplinar o fornecimento de informações de contribuintes do ICMS, estipulou cláusulas envolvendo o tratamento de dados pessoais que não guardam correlação com o fato gerador do imposto. As regras sobre o fornecimento de dados são genéricas e permitem o compartilhamento sem qualquer procedimento administrativo prévio.

O convênio vai de encontro à tese fixada no julgamento da ADI nº 2.859 no que concerne ao regramento sobre a transmissão dos dados fiscais sigilosos, haja vista que não foram observados os requisitos para a automaticidade da transmissão de informações pelas instituições bancárias aos Estados e Municípios.

Não se pensou em uma regulamentação específica para esses Entes Federativos que dispusesse sobre: a pertinência temática entre as informações bancárias requeridas e o tributo objeto de cobrança no processo administrativo instaurado, a prévia notificação do contribuinte quanto à instauração do processo administrativo de requisição de informações sobre sua movimentação financeira e relativamente a todos os demais atos, a submissão do pedido de acesso ao crivo de um superior hierárquico do agente fiscal requerente, o uso de sistemas eletrônicos de segurança certificados e com registro de acesso, a implementação de mecanismos efetivos de apuração e de correção de desvios e o “amplo acesso do contribuinte aos autos, garantindo-lhe a extração de cópias de quaisquer documentos e decisões, de maneira a permitir que possa exercer a todo tempo o

²⁸³ Prazo, finalidade específica, pertinência da requisição etc.

controle jurisdicional dos atos da administração”²⁸⁴.

Posteriormente, discorreu-se especificamente sobre as prescrições relacionadas à proteção de dados pessoais. Nesse contexto, destacou-se que a norma prevê o princípio do livre acesso, que garante, aos titulares, uma “consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais” (art. 6º, inciso IV). Adicionalmente, o art. 9º prescreve, objetivamente, as informações que deverão ser fornecidas ao titular dos dados: finalidade específica, forma e duração do tratamento, identificação e contato do controlador, informações sobre o uso compartilhado, responsabilidade dos agentes envolvidos e direitos do titular.

Além dessas diretrizes, o *caput* do referido dispositivo observa que “outras características” poderão ser previstas em regulamentação para o atendimento do princípio do livre acesso. Nesse ponto, a LGPD possibilitou a idealização de uma normatização própria para o direito à autodeterminação informativa, o que permitiria uma melhor instrumentalização dessa garantia. Dessa forma, seria salutar que o Poder Legislativo estipulasse normas procedimentais para o princípio do livre acesso, bem assim regulamentando a sua aplicação em relação ao tratamento de dados pelo Poder Público.

Vale mencionar, ainda, consoante o princípio do livre acesso, a previsão do art. 18, que confere ao titular o direito de requerer ações e informações do controlador a qualquer momento. Sendo o controlador, na definição da LGPD, a “pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais”, conclui-se que a Fazenda Pública deve observar essa regra.

Nessa perspectiva, o contribuinte poderia, a princípio, solicitar a confirmação da existência de tratamento, o acesso aos dados, a correção de dados incompletos, inexatos ou desatualizados, a anonimização, o bloqueio ou a eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a lei, a exclusão de dados pessoais, mesmo que tratados com o seu consentimento, as informações sobre o compartilhamento com outras entidades etc.

Todavia, verifica-se, de plano, que algumas dessas garantias, expressamente elencadas no art. 18 da LGPD, se lidas em sua literalidade, poderiam obstar a

²⁸⁴ BRASIL, ref. 87.

própria atividade tributária. É que a eliminação de um dado utilizado em uma fiscalização procedida pelo Fisco poderia, inclusive, elidir a tributação. Da mesma forma, como visto, há hipóteses em que o acesso aos dados, pelo titular, poderia contaminar o procedimento fiscalizatório, uma vez que tal permissão possibilitaria que o contribuinte tomasse ciência do que a Administração Tributária já saberia sobre suas operações e, assim, desfizesse ou camuflasse os possíveis fatos geradores.

Com essas considerações, nota-se que não há como pretender uma simples sobreposição dos dispositivos da LGPD no Sistema Tributário brasileiro. Isso reforça a necessidade de um regramento específico em relação à aplicação do princípio do livre acesso no setor público, notadamente nas relações jurídico-tributárias.

Não obstante, importante lembrar que há um dever mínimo de informação. Conforme o art. 23 da LGPD, é obrigatório o fornecimento – em veículos de fácil acesso, preferencialmente sítios eletrônicos – de informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para o tratamento de dados pelo Fisco.

Mais adiante, foi trazido o panorama nacional e internacional acerca dos *standards* fixados nas operações de coleta e transferência de dados pela Fazenda Pública. Primeiramente, foram debatidos os critérios definidos no julgamento conjunto do referendo de medida cautelar concedida nas ADIs nº 6387, nº 6388, nº 6389, nº 6390 e nº 6393, que tratavam do exame de constitucionalidade da MP nº 954/2020. A norma determinava a coleta compulsória de dados de usuários de telefonia para repasse ao IBGE, que pretendia realizar pesquisas domiciliares em caráter não presencial.

Nesse caso, considerando a ausência de precisão da norma, que fundamentava o uso de dados com o argumento de “produção estatística oficial”, entendeu a Corte que não havia a garantia de requisitos de transparência que assegurassem o nível mínimo de controle sobre os dados. Assim, a Medida Provisória deixava de proporcionar, ao titular dos dados, as condições necessárias ao monitoramento do uso de suas informações.

Outrossim, na ADI nº 6.649 e na ADPF nº 695, o STF conferiu interpretação conforme a Constituição Federal ao Decreto nº 10.046/2019, a fim de assegurar que o compartilhamento de dados entre órgãos e entidades da Administração Pública pressupõe a eleição de propósitos legítimos, específicos e explícitos para o

tratamento de dados, a compatibilidade do tratamento com as finalidades informadas e a restrição do compartilhamento ao mínimo necessário para o atendimento do objetivo apontado.

Dessa forma, determinou o Tribunal que a transmissão de dados entre órgãos públicos exige a observância do art. 23, inciso I, da LGPD. Novamente, o Supremo prestigiou a regra insculpida nesse importante dispositivo, que regula, no âmbito do tratamento de dados pessoais pelas pessoas jurídicas de direito público, o dever de informação detalhada da operação. Complementarmente a esse dever de publicidade, assentou-se, no acórdão, a possibilidade de responsabilização por ato de improbidade administrativa, caso haja transgressão dolosa da obrigação (art. 11, inciso IV, da LIA).

Por derradeiro, também merecem destaque as balizas desenhadas pela Corte em relação ao Comitê Central de Governança de Dados. Segundo a decisão, cabe ao CCGD a previsão de mecanismos rigorosos de controle de acesso ao CBC, que deve ficar limitado a “órgãos e entidades que comprovarem real necessidade de acesso aos dados pessoais nele reunidos”. Com isso, condicionou-se a permissão de acesso à existência de propósitos legítimos, específicos e explícitos, orientados pelo exame da imprescindibilidade da informação para o atendimento do interesse público.

A fim de parametrizar essas condicionantes, o STF determinou que o comitê precisaria justificar, de maneira formal, prévia e minudentemente, a necessidade de inclusão de novos dados pessoais na base integradora e a escolha das bases temáticas a serem inseridas no Cadastro Base. Também foi imposta a elaboração de medidas de segurança, especialmente a criação de um sistema eletrônico de registro de acesso para apurar eventuais de responsabilizações de agentes.

Além disso, definiu-se, com esse precedente, que o CCGD deve contar com uma composição plural e independente, isto é, que dele participem representantes externos à Administração Pública. Nessa linha, a esses membros devem ser asseguradas garantias mínimas contra influências indevidas.

Após a instituição de assentos destinados a membros da sociedade civil, o CCGD conta, hoje, com uma composição plural e tem desenvolvido inúmeros trabalhos voltados à deliberação sobre as orientações e as diretrizes para a

integração dos órgãos e das entidades com o CBC²⁸⁵.

Destaca-se, nesse cenário, a publicação da Resolução CCGD nº 11, de 22 de junho de 2022²⁸⁶, que instituiu o Subcomitê Técnico de Governança de Dados, responsável pela proposição de orientações para estruturação da Governança de Dados dos órgãos e das entidades da Administração Pública federal direta, autárquica e fundacional e dos demais Poderes da União, conforme o art. 1º do Decreto nº 10.046/2019. Com isso, surge mais um fórum para a promoção dos debates em relação às competências da Administração Tributária em matéria de compartilhamento de dados.

Seguidamente, falou-se sobre a tese fixada no Tema 990 da repercussão geral. O Supremo julgou constitucional o envio da íntegra dos processos fiscais ao Ministério Público, sem prévia autorização judicial, desde que respeitado o sigilo das informações. Prevaleceu a corrente do Ministro Alexandre de Moraes, que buscou conciliar as diferentes posições apresentadas pelos membros da Corte.

A despeito do entendimento esposado no voto condutor, no sentido de considerar lícitas e compartilháveis todas as informações e os dados constantes no procedimento de fiscalização, não se pode perder de vista as preocupações externadas pelos demais Ministros, a exemplo do Ministro Gilmar Mendes, que sugeriu a fixação de tese determinando que, no encaminhamento da Representação Fiscal para Fins Penais, seria apenas permitido o compartilhamento dos documentos “absolutamente imprescindíveis para a persecução penal”. Da mesma forma, o relator, Ministro Dias Toffoli, refletiu sobre a importância de se evitar o fornecimento de dados pessoais estranhos à apuração do ilícito penal, a fim de se resguardar a garantia da privacidade.

Afinal, em uma das teses firmadas pelo Tribunal, impõe-se o “estabelecimento de instrumentos efetivos de apuração e correção de eventuais desvios”. Dessa maneira, o uso irrestrito de dados para finalidades alheias à persecução penal definida no procedimento de representação fiscal certamente configuraria um desvio a ser corrigido.

À vista disso, também foram exploradas as penalidades às quais os agentes

²⁸⁵ Disponível em: <https://www.gov.br/governodigital/pt-br/governanca-de-dados/comite-central-de-governanca-de-dados>. Acesso em: 25 jul. 2023.

²⁸⁶ BRASIL. Comitê Central de Governança de Dados. **Resolução CCGD nº 11, de 22 de junho de 2022**. Diário Oficial da União, Brasília, DF, 27 jun. 2022, edição 119, seção 2, p. 18. Disponível em: <https://www.in.gov.br/en/web/dou/-/resolucao-ccgd-n-11-de-22-de-junho-de-2022-410418736>. Acesso em: 25 jul. 2023.

públicos envolvidos nas operações com dados estão sujeitos. Como visto, o art. 325 do Código Penal brasileiro disciplina o crime de violação de sigilo funcional, descrito como a conduta de revelação de “fato de que tem ciência em razão do cargo e que deva permanecer em segredo, ou facilitar-lhe a revelação”. Incorre igualmente nesse delito quem atribui, fornece ou empresta senha ou qualquer outro meio que facilite ou permita o acesso de pessoas não autorizadas às bases da Administração Pública ou faça uso indevido do acesso restrito.

Já o art. 132, inciso IX, da Lei nº 8.112/1990 e o art. 6º da Portaria RFB nº 2.344/2011 preveem que o ato de “revelação de segredo do qual se apropriou em razão do cargo” atrai a aplicação da penalidade de demissão. A conduta, como anteriormente abordado, também configura improbidade administrativa, nos moldes do art. 11, inciso III, da LIA.

O servidor também pode responder judicialmente, em ação de reparação de danos morais e materiais pela violação do sigilo. Além disso, se não agir em prol do interesse público, visando alcançar a finalidade pretendida pela Administração com base em seu dever funcional, o agente público também será responsabilizado.

Por fim, pontuou-se que a LGPD delegou à ANPD a tarefa de elaborar relatório dispondo sobre as medidas cabíveis para fazer cessar a violação em caso de infração à lei decorrente do tratamento de dados pessoais por órgãos públicos (art. 31). A autoridade nacional também tem a tarefa de alertar os órgãos de controle interno se houver descumprimento da lei pelo Poder Público (art. 55-J, inciso XXII). Considerando essa expressa atribuição de competência para fiscalizar as atividades dos órgãos públicos, a ANPD assume relevante papel na imposição de freios à atuação dos órgãos tributários.

Diante dessas considerações, a fim de trazer subsídios comparativos ao debate, o trabalho também discorreu sobre a abordagem do tema a nível internacional. Foram destacados os principais pontos do relatório “*The Path to Becoming a Data-Driven Public Sector*”, da OCDE, que propõe algumas recomendações para que os países possam aprimorar seus mecanismos internos, em busca de um “setor público movido a dados” (*Data-Driven Public Sector – DDPS*).

Em seguida, foi estudado o Sistema Tributário alemão, com enfoque nas recentes inovações legislativas que buscaram estabelecer um diálogo entre o RGPD e as regras do Código Tributário daquele país. Nesse contexto, constatou-se a

necessidade de se equilibrar a atividade fiscalizatória com o direito do titular de ser informado, porque os preceitos insculpidos no AO são vagos e acabam por permitir uma supressão da privacidade, em nome da eficiência administrativo-tributária.

Aliás, esse problema destoa das razões exprimidas pela Corte Constitucional alemã no julgamento do 1 BvR 2388/03. No caso, o BVerfG determinou que o interesse do contribuinte não pode ser considerado menos importante do que o objetivo de cobrança igualitária de tributos buscado pela manutenção do sigilo em relação ao próprio titular dos dados.

Nesse sentido, a dispensa de comunicação com o contribuinte sobre o tratamento realizado deveria ser uma exceção e, por se tratar de regra que impõe severas limitações ao direito à autodeterminação informativa, é imprescindível que seja sempre garantido que a coleta e o armazenamento de dados estejam corretos. Em outras palavras, o titular não pode sofrer desvantagens por conta do impedimento legal de acesso às suas informações, devendo a operação seguir estritamente as normas que regem o rito de apuração de obrigações tributárias.

Demais disso, a *Grand Chamber* do TEDH, ao julgar o caso *L.B. v. Hungary*, concluiu que a política de divulgação da lista de “grandes devedores” seria desproporcional à luz do direito à privacidade – em violação ao art. 8º da CEDH – e com base no princípio de minimização do uso de dados pessoais. Nessa perspectiva, foi feita importante ponderação quanto à possibilidade da adoção de medidas menos restritivas pelo Fisco, que pudessem evitar graves impactos à intimidade dos contribuintes inadimplentes e, paralelamente, alcançar as finalidades arrecadatórias do interesse público.

No caso *James Harper v. Charles P. Rettig*, por seu turno, a Corte de Apelações americana do Primeiro Circuito determinou que o titular dos dados tem o direito de recorrer ao Judiciário em controvérsias que tratem sobre a coleta de informações do contribuinte realizada pela IRS. O tribunal concluiu que, nos casos em que o processo não versar sobre pleito contrário ao tributo em si, mas, sim, sobre a oposição aos mecanismos utilizados pelo Fisco americano para a obtenção de informações, é legítima a postulação em juízo. A decisão foi um importante passo no sentido da contenção de excessos praticados pelas autoridades, ao submeter ao crivo do Poder Judiciário as questões sobre eventuais abusos no tratamento de dados pessoais pelo órgão tributário.

Todas essas questões examinadas permitem concluir que os problemas existentes no atual Sistema Tributário brasileiro exigem uma abordagem focada na abertura da ordem constitucional às transformações tecnológicas. Afinal, a atual conjuntura permitiu conceber a ideia de um direito fundamental à proteção de dados, hoje expressamente previsto na Constituição Federal (art. 5º, inciso LXXIX, da CF).

Trata-se de leitura do texto maior como “algo que se realiza no tempo, e não um dado inerte”²⁸⁷. Os desenvolvimentos decorrentes do avanço do ambiente digital exigem que os novos dispositivos infraconstitucionais, que dispõem sobre as atuais relações entre contribuinte e agente público, sejam interpretados em consonância com as normas superiores, tal qual se fez nos julgamentos citados nos capítulos anteriores.

Nessa linha de ideias, a eficiência que se demanda da Administração Pública, notadamente do agente fiscal no âmbito da arrecadação de tributos – o que é albergado pelo interesse público – deve ser compreendida “no contexto de um conjunto mais amplo de princípios e como elementos integrantes do compromisso que o Estado deve ter com a democracia e com a concretização de direitos fundamentais”²⁸⁸.

Diante dos desafios abordados nesta pesquisa, verifica-se que há, atualmente, a necessidade de se atualizar e reconceitualizar a força normativa da Carta Magna brasileira, a fim de se preservar garantias individuais que eventualmente sejam ameaçadas pelo descompasso entre a proteção da intimidade e o poder de vigilância. Assim, ao passo que as tecnologias oferecem novas oportunidades à sociedade da informação, deve-se ter em mente os potenciais poderes de comunicação e de poder econômico, que podem impor interesses de forma seletiva pela manipulação ou por outros meios²⁸⁹.

Como bem pontuado pelo Ministro Gilmar Mendes no julgamento paradigmático do referendo de medida cautelar concedida nas ADIs nº 6387, nº 6388, nº 6389, nº 6390 e nº 6393, “vivemos na era das escolhas de Sofia automatizadas”. Nesse sentido, reconheceu o Ministro que “para muito além do mero debate sobre o sigilo comunicacional, [...] [o Supremo Tribunal Federal] deve

²⁸⁷ BRASIL, ref. 126.

²⁸⁸ WIMMER, 2021, p. 278.

²⁸⁹ HOFFMANN-RIEM, Wolfgang. Innovaciones en la jurisprudencia del Tribunal Constitucional Alemán, a propósito de la garantía de los derechos fundamentales en respuesta a los cambios que conducen a la Sociedad de la Información. **Direito Público**, v. 12, n. 64, p. 40-61, jul./ago. 2015. p. 48-49.

reconhecer que a disciplina jurídica do processamento e da utilização da informação acaba por afetar o sistema de proteção de garantias individuais como um todo”²⁹⁰.

No entanto, como bem ressaltado por Thomas Feltzer e Christopher Yoo, parcela considerável da literatura constitucional ainda não confere a mesma atenção ao impacto que inovações tecnológicas podem gerar nessas discussões²⁹¹:

O que tem recebido menor atenção é a dimensão pela qual mudanças na interpretação constitucional são movidas não por alterações nos costumes políticos, mas sim pelo desenvolvimento de novas tecnologias [...] [Ocorre que] a melhor compreensão sobre os impactos potencialmente causados por novas tecnologias [na interpretação constitucional] pode resultar em uma análise mais aprofundada acerca da evolução do direito constitucional ao longo do tempo (tradução nossa).

Em sentido convergente, Gilmar Ferreira Mendes e Victor Oliveira Fernandes propõem uma “transformação teórica da jurisdição constitucional brasileira voltada à proteção de direitos fundamentais no ciberespaço”, sobretudo diante da “natural abertura” dos textos normativos e da “incapacidade de antecipação legislativa dos problemas relacionados ao uso das novas tecnologias”²⁹².

É fundamental, nessa perspectiva, a “compreensão da disciplina de proteção de dados pessoais como meio de tutela da personalidade do cidadão, garantindo tanto a autonomia das suas escolhas como a sua proteção contra situações potencialmente discriminatórias²⁹³. No âmbito do tratamento de dados para fins tributários, essa abordagem também deve ser direcionada para a nova leitura que se faz do direito à privacidade do contribuinte como um “autopoder informativo”.

Foi citado, nesse sentido, que a LGPD trouxe a possibilidade de o legislador posteriormente regulamentar o princípio do livre acesso, o que poderia ser pensado também para as atividades relacionadas à fiscalização de obrigações fiscais (art. 9º). Da mesma forma, o CCGD, com base em sua competência para articular políticas

²⁹⁰ BRASIL, ref. 199.

²⁹¹ No original: “*What has received less attention is the extent which changes in constitutional interpretation are driven not by shifts in political mores, but rather by new developments in technology [...] A better understanding of the potential impact of new technologies should provide a deeper appreciation of the manner in which constitutional law evolves over time*”. FETZER, Thomas; YOO, Christopher S. *New Technologies and Constitutional Law. Faculty Scholarship at Penn Law*, n. 545, 2012, p. 1-2.

²⁹² MENDES, Gilmar Ferreira; FERNANDES, Victor Oliveira. Constitucionalismo digital e jurisdição constitucional: uma agenda de pesquisa para o caso brasileiro. *Revista Brasileira de Direito*, Passo Fundo, v. 16, n. 1, p. 1-33, jan./abr., 2020. p. 3.

²⁹³ MENDES, Laura Schertel Ferreira. *Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental*. São Paulo: Saraiva, 2014. p. 37.

de governança no bojo da troca de informações entre órgãos e entidades da Administração Pública, poderá trazer as operações tributárias para o debate.

A partir de soluções como essas, algumas das medidas existentes, previstas em normas procedimentais da RFB, poderiam ser mais bem adequadas, com suporte nos parâmetros legais, às normas de proteção de dados pessoais.

O desafio também exigirá do Poder Judiciário, notadamente do STF, um olhar calcado na força normativa da Constituição em face das inovações tecnológicas. Todavia, esse olhar, como adverte Cass Sunstein, precisa ser cauteloso: em um período de rápidas mudanças, marcado por incertezas tecnológicas, exige-se que se pense o ciberespaço com uma “cautela constitucional”, porque os valores decorrentes dessa nova realidade estão em constante fluxo e não são de simples classificação²⁹⁴.

Vale lembrar que não se defende, nesta pesquisa, que o contribuinte possua um direito à “autodeterminação informativa fiscal”, como se a ele fosse dado o poder de rejeitar a atuação do agente tributário. Essa atividade é plenamente vinculada e, em nome do princípio da igualdade tributária, ao Estado deve ser conferido o acesso aos dados dos cidadãos e das empresas²⁹⁵. Por isso, inclusive, que se alertou sobre a incompatibilidade de alguns dos dispositivos da LGPD – a exemplo do art. 18 – com as atribuições do Fisco brasileiro.

O que se pretende é propor um modelo com nível adequado e satisfatório de proteção, que ainda não foi implementado nem internamente nem a nível global²⁹⁶. Na mesma linha da lição de Roman Seer acerca da incompatibilidade da “estocagem de informações pessoais protegidas pelos direitos fundamentais com finalidade indeterminada ou ainda não determinável” com a Lei Fundamental alemã²⁹⁷, o padrão atual, como se pôde perceber, também não se harmoniza com as garantias previstas na Constituição Federal de 1988, notadamente os direitos à privacidade e à proteção de dados.

Assim, para que se siga um modelo alinhado ao texto constitucional e às diretrizes internacionais, é imprescindível que os pontos acima indicados sejam trazidos para o diálogo. Esse debate, travado nesta pesquisa, contudo, está ainda

²⁹⁴ SUNSTEIN, Cass R. Constitutional Caution. **University of Chicago Legal Forum**, v. 361, p. 361-375, 1996.

²⁹⁵ SEER, 2020, p. 24.

²⁹⁶ Cf. LIOTTI, 2022, p. 158.

²⁹⁷ SEER, *op. cit.*, p. 25.

em desenvolvimento, ante a incipiente implementação das regras de proteção de dados e, por consequência, do novo aparato burocrático referente ao monitoramento das questões subjacentes. Ainda é necessário manter-se vigilante em relação às vicissitudes que surgirão com a regulamentação e o supervisionamento das relações jurídico-tributárias nesse novo ambiente digital.

REFERÊNCIAS

AFONSO, José Roberto; ARDEO, Thaís; MOTTA, Bernardo. Impactos da Revolução Digital na Tributação: uma primeira revisão bibliográfica. *In*: AFONSO, José Roberto; SANTANA, Hadassah Laís (Orgs.). **Tributação 4.0**. São Paulo: Almedina, 2020. p. 217-226.

AGUIAR, Luciana Ibiapina Lira. Tributação de marketing digital por meio de *websites*: Caso *Google AdWords* e o contraponto entre as perspectivas brasileira e internacional. *In*: FARIA, Renato Vilela; SILVEIRA, Ricardo Maitto da; MONTEIRO, Alexandre Luiz Moraes do Rêgo (Orgs.). **Tributação da Economia Digital**: Desafios no Brasil, experiência internacional e novas perspectivas. São Paulo: Saraiva Educação, 2018. p. 570-587.

ALEMANHA. Bundesministerium der Finanzen. **The Fiscal Code of Germany**. Fiscal Code of Germany in the version promulgated on 1 October 2002 (Federal Law Gazette [Bundesgesetzblatt] I p. 3866; 2003 I p. 61), last amended by Article 17 of the Act of 17 July 2017 (Federal Law Gazette I p. 2541). Disponível em: https://www.gesetze-im-internet.de/englisch_ao/. Acesso em: 20 maio 2023.

ALEMANHA. Bundesverfassungsgericht. **1 BvR 2388/03**. BverfGE, n. 120, 2008. Disponível em: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2008/03/rs20080310_1bvr238803.htm . Acesso em: 20 maio 2023.

ALEMANHA. **Lei Fundamental da República Federal da Alemanha, de 23 de maio de 1949**. Berlim: Parlamento Federal Alemão, [2019]. Disponível em: <https://www.bundestag.de/pt>. Acesso em: 5 out. 2023.

AMARO, Luciano. **Direito Tributário Brasileiro**. São Paulo: Saraiva, 22. ed., 2017.

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

BLACK, Gillian; STEVENS, Leslie. Enhancing data protection and data processing in the public sector: the critical role of proportionality and the public interest. **SCRIPTed**, v. 10, n. 1, p. 93-122, 2013.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988**. Brasília: Presidência da República, [2022]. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm. Acesso em: 24 fev. 2023.

BRASIL. Câmara dos Deputados. **Proposta de Emenda à Constituição nº 45, de 2019**. Altera o Sistema Tributário Nacional e dá outras providências. Brasília, DF, [2019]. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2196833>. Acesso em: 23 jun. 2023.

BRASIL. Comitê Central de Governança de Dados. **Resolução CCGD nº 11, de 22 de junho de 2022**. Diário Oficial da União, Brasília, DF, 27 jun. 2022, edição 119,

seção 2, p. 18. Disponível em: <https://www.in.gov.br/en/web/dou/-/resolucao-ccgd-n-11-de-22-de-junho-de-2022-410418736>. Acesso em: 25 jul. 2023.

BRASIL. Conselho Nacional de Política Fazendária. **Ato COTEPE/ICMS nº 65, de 19 de dezembro de 2018**. Dispõe sobre as especificações técnicas para a geração de arquivos referentes às informações prestadas por instituições e intermediadores financeiros e de pagamento, integrantes ou não do Sistema de Pagamentos Brasileiro – SPB, relativas às transações com cartões de débito, crédito, de loja (*private label*), transferência de recursos, transações eletrônicas do Sistema de Pagamento Instantâneo e demais instrumentos de pagamento eletrônicos [...]. Brasília, DF, [2018]. Disponível em: <https://www.confaz.fazenda.gov.br/legislacao/atos/2018/ato-cotepe-icms-65-18>. Acesso em: 13 mar. 2023.

BRASIL. Conselho Nacional de Política Fazendária. **Convênio ICMS nº 134, de 9 de dezembro de 2016**. Dispõe sobre o fornecimento de informações prestadas por instituições e intermediadores financeiros e de pagamento, integrantes ou não do Sistema de Pagamentos Brasileiro – SPB, relativas às transações com cartões de débito, crédito, de loja (*private label*), transferência de recursos, transações eletrônicas do Sistema de Pagamento Instantâneo e demais instrumentos de pagamento eletrônicos [...]. Brasília, DF, [2016]. Disponível em: https://www.confaz.fazenda.gov.br/legislacao/convenios/2016/CV134_16. Acesso em: 13 mar. 2023.

BRASIL. Conselho Nacional de Política Fazendária. **Convênio ICMS nº 166, de 23 de setembro de 2022**. Altera o Convênio ICMS nº 134/16, que dispõe sobre o fornecimento de informações prestadas por instituições e intermediadores financeiros e de pagamento, integrantes ou não do Sistema de Pagamentos Brasileiro – SPB, relativas às transações com cartões de débito, crédito, de loja (*private label*), transferência de recursos, transações eletrônicas do Sistema de Pagamento Instantâneo e demais instrumentos de pagamento eletrônicos [...]. Brasília, DF, [2022]. Disponível em: https://www.confaz.fazenda.gov.br/legislacao/convenios/2022/CV166_22. Acesso em: 13 mar. 2023.

BRASIL. **Decreto nº 10.046, de 9 de outubro de 2019**. Dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados. Brasília: Presidência da República, [2019]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D10046.htm. Acesso em: 13 mar. 2023.

BRASIL. **Decreto nº 10.209, de 22 de janeiro de 2020**. Dispõe sobre a requisição de informações e documentos e sobre o compartilhamento de informações protegidas pelo sigilo fiscal. Brasília: Presidência da República, [2020]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/d10209.htm. Acesso em: 13 maio 2023.

BRASIL. **Decreto nº 11.266, de 25 de novembro de 2022**. Altera o Decreto nº 10.046, de 9 de outubro de 2019, 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. Brasília: Presidência da República, [2022]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2022/Decreto/D11266.htm#art1. Acesso em: 13 mar. 2023.

BRASIL. **Decreto nº 3.724, de 10 de janeiro de 2001**. Regulamenta o art. 6º da Lei Complementar nº 105, de 10 de janeiro de 2001, relativamente à requisição, acesso e uso, pela Secretaria da Receita Federal, de informações referentes a operações e serviços das instituições financeiras e das entidades a elas equiparadas. Brasília: Presidência da República, [2001]. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto/2001/d3724.htm#:~:text=DECRETO%20N%C2%BA%203.724%2C%20DE%2010%20DE%20JANEIRO%20DE%202001.&text=Regulamenta%20o%20art.,das%20entidades%20a%20elas%20equiparadas. Acesso em: 24 maio 2023.

BRASIL. **Decreto nº 8.789, de 29 de junho de 2016**. Dispõe sobre o compartilhamento de bases de dados na administração pública federal. Brasília: Presidência da República, [2016]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8789.htm. Acesso em: 13 mar. 2023.

BRASIL. **Decreto nº 8.842, de 29 de agosto de 2016**. Promulga o texto da Convenção sobre Assistência Mútua Administrativa em Matéria Tributária emendada pelo Protocolo de 1º de junho de 2010, firmada pela República Federativa do Brasil em Cannes, em 3 de novembro de 2011. Brasília: Presidência da República, [2016]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/D8842.htm. Acesso em: 24 fev. 2023.

BRASIL. **Decreto-lei nº 2.848, de 7 de dezembro de 1940**. Código Penal. Brasília: Presidência da República, [1940]. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 6 maio 2023.

BRASIL. **Lei Complementar nº 105, de 10 de janeiro de 2001**. Dispõe sobre o sigilo das operações de instituições financeiras e dá outras providências. Brasília: Presidência da República, [2001]. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/lcp/lcp105.htm. Acesso em: 24 fev. 2023.

BRASIL. **Lei nº 5.172, de 25 de outubro de 1966**. Dispõe sobre o Sistema Tributário Nacional e institui normas gerais de direito tributário aplicáveis à União, Estados e Municípios. Brasília: Presidência da República, [1966]. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l5172.htm. Acesso em: 24 fev. 2023.

BRASIL. **Lei nº 8.112, de 11 de dezembro de 1990**. Dispõe sobre o regime jurídico dos servidores públicos civis da União, das autarquias e das fundações públicas federais. Brasília: Presidência da República, [1991]. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8112cons.htm. Acesso em: 24 fev. 2023.

BRASIL. **Lei nº 8.429, de 2 de junho de 1992**. Dispõe sobre as sanções aplicáveis em virtude da prática de atos de improbidade administrativa, de que trata o § 4º do art. 37 da Constituição Federal; e dá outras providências. Brasília: Presidência da

República, [1992]. Disponível em:

https://www.planalto.gov.br/ccivil_03/leis/l8429.htm. Acesso em: 20 maio 2023.

BRASIL. **Lei nº 9.613, de 3 de março de 1998**. Dispõe sobre os crimes de “lavagem” ou ocultação de bens, direitos e valores; a prevenção da utilização do sistema financeiro para os ilícitos previstos nesta Lei; cria o Conselho de Controle de Atividades Financeiras – COAF, e dá outras providências. Brasília: Presidência da República, [1998]. Disponível em:

https://www.planalto.gov.br/ccivil_03/leis/l9613.htm. Acesso em: 20 maio 2023.

BRASIL. **Lei nº 10.174, de 9 de janeiro de 2001**. Altera o art. 11 da Lei no 9.311, de 24 de outubro de 1996, que institui a Contribuição Provisória sobre Movimentação ou Transmissão de Valores e de Crédito e Direitos de Natureza Financeira – CPMF, e dá outras providências. Brasília: Presidência da República, [2001]. Disponível em: https://www.planalto.gov.br/ccivil_03/Leis/LEIS_2001/L10174.htm. Acesso em: 24 fev. 2023.

BRASIL. **Lei nº 12.527, de 18 de novembro de 2011**. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Brasília: Presidência da República, [2011]. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2011/Lei/L12527.htm#art1. Acesso em: 5 mar. 2023.

BRASIL. **Lei nº 13.254, de 13 de janeiro de 2016**. Dispõe sobre o Regime Especial de Regularização Cambial e Tributária (RERCT) de recursos, bens ou direitos de origem lícita, não declarados ou declarados incorretamente, remetidos, mantidos no exterior ou repatriados por residentes ou domiciliados no País. Brasília: Presidência da República, [2016]. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2016/Lei/l13254.htm. Acesso em: 24 fev. 2023.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília: Presidência da República, [2018]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 24 fev. 2023.

BRASIL. **Lei nº 14.129, de 29 de março de 2021**. Dispõe sobre princípios, regras e instrumentos para o Governo Digital e para o aumento da eficiência pública e altera a Lei nº 7.116, de 29 de agosto de 1983, a Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), a Lei nº 12.682, de 9 de julho de 2012, e a Lei nº 13.460, de 26 de junho de 2017. Brasília: Presidência da República, [2021]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/Lei/L14129.htm. Acesso em: 27 fev. 2023.

BRASIL. **Medida Provisória nº 954, de 2020**. Dispõe sobre o compartilhamento de dados por empresas de telecomunicações prestadoras de Serviço Telefônico Fixo Comutado e de Serviço Móvel Pessoal com a Fundação Instituto Brasileiro de Geografia e Estatística, para fins de suporte à produção estatística oficial durante a situação de emergência de saúde pública de importância internacional decorrente do coronavírus (covid-19), de que trata a Lei nº 13.979, de 6 de fevereiro de 2020.

Brasília: Presidência da República, [2020]. Disponível em:

<https://www.congressonacional.leg.br/materias/medidas-provisorias/-/mpv/141619>.

Acesso em: 10 maio 2023.

BRASIL. Secretaria Especial da Receita Federal do Brasil. **Instrução Normativa SRF nº 19, de 17 de fevereiro de 1998**. Disciplina os procedimentos de fornecimento de dados cadastrais e econômico-fiscais da Secretaria da Receita Federal - SRF, a outras entidades. Diário Oficial da União, Brasília, DF, 18 fev. 1998, seção 1, p. 19. Disponível em:

<http://normas.receita.fazenda.gov.br/sijut2consulta/link.action?visao=anotado&idAto=13242>. Acesso em: 24 fev. 2023.

BRASIL. Secretaria Especial da Receita Federal do Brasil. **Instrução Normativa SRF nº 165, 10 de junho de 2002**. Aprova o Programa de Atendimento à Requisição de Informações sobre Movimentação Financeira (PA-RMF). Diário Oficial da União, Brasília, DF, 12 jun. 2002, seção 1, p. 18. Disponível em:

<http://normas.receita.fazenda.gov.br/sijut2consulta/link.action?idAto=15017&visao=anotado>. Acesso em: 24 maio 2023.

BRASIL. Secretaria Especial da Receita Federal do Brasil. **Portaria RFB nº 34, de 14 de maio de 2021**. Dispõe sobre o compartilhamento de dados não protegidos por sigilo fiscal com órgãos e entidades da Administração Pública Federal direta, autárquica e fundacional e dos demais Poderes da União. Diário Oficial da União, Brasília, DF, 18 maio 2021, seção 1, p. 64. Disponível em:

<http://normas.receita.fazenda.gov.br/sijut2consulta/link.action?idAto=117598>. Acesso em: 18 maio 2023.

BRASIL. Secretaria Especial da Receita Federal do Brasil. **Portaria RFB nº 81, de 11 de novembro de 2021**. Aprova o sistema Compartilha Receita Federal e estabelece regras para o fornecimento, a terceiros, de dados e informações no interesse de seus titulares. Diário Oficial da União, Brasília, DF, 1º dez. 2021, seção 1-B, p. 1. Disponível em:

<http://normas.receita.fazenda.gov.br/sijut2consulta/link.action?idAto=12189090>.

Acesso em: 18 jun. 2023.

BRASIL. Secretaria Especial da Receita Federal do Brasil. **Portaria RFB nº 167, de 14 de abril de 2022**. Autoriza o Serviço Federal de Processamento de Dados a disponibilizar acesso, para terceiros, dos dados e informações que especifica. Diário Oficial da União, Brasília, DF, 19 abr. 2022, seção 1, p. 51. Disponível em:

<http://normas.receita.fazenda.gov.br/sijut2consulta/link.action?idAto=123666>. Acesso em: 18 maio 2023.

BRASIL. Secretaria Especial da Receita Federal do Brasil. **Portaria RFB nº 229, de 26 de fevereiro de 2013**. Institui o Comitê de Tecnologia e Segurança da Informação no âmbito da Secretaria da Receita Federal do Brasil e dá outras providências. Diário Oficial da União, Brasília, DF, 27 fev. 2013, seção 1, p. 91. Disponível em:

<http://normas.receita.fazenda.gov.br/sijut2consulta/link.action?naoPublicado=&idAto=39727&visao=anotado>. Acesso em: 18 maio 2023.

BRASIL. Secretaria Especial da Receita Federal do Brasil. **Portaria RFB nº 551, de 30 de abril de 2013**. Dispõe sobre o tratamento de expedientes oriundos de outros órgãos, entidades, autoridades ou cidadãos utilizados para solicitar dados econômico-fiscais de contribuintes, análise de situação fiscal ou instauração de procedimento fiscal no âmbito da RFB, inclusive no que se refere à preservação do caráter sigiloso de informações protegidas por sigilo fiscal. BP/MF, Brasília, DF, 3 maio 2013. Disponível em: <http://normas.receita.fazenda.gov.br/sijut2consulta/link.action?visao=anotado&idAto=70296>. Acesso em: 24 fev. 2023.

BRASIL. Secretaria Especial da Receita Federal do Brasil. **Portaria RFB nº 1.750, de 12 de novembro de 2018**. Dispõe sobre representação fiscal para fins penais referente a crimes contra a ordem tributária, contra a Previdência Social, e de contrabando ou descaminho, sobre representação para fins penais referente a crimes contra a Administração Pública Federal, em detrimento da Fazenda Nacional ou contra administração pública estrangeira, de falsidade de títulos, papéis e documentos públicos e de “lavagem” ou ocultação de bens, direitos e valores, e sobre representação referente a atos de improbidade administrativa. Diário Oficial da União, Brasília, DF, 14 nov. 2018, seção 1, p. 57. Disponível em: <http://normas.receita.fazenda.gov.br/sijut2consulta/link.action?idAto=96434>. Acesso em: 18 maio 2023.

BRASIL. Secretaria Especial da Receita Federal do Brasil. **Portaria RFB nº 2.344, de 24 de março de 2011**. Disciplina o acesso a informações protegidas por sigilo fiscal constantes de sistemas informatizados da Secretaria da Receita Federal do Brasil. Diário Oficial da União, Brasília, DF, 28 mar. 2011, seção 1, p. 33. Disponível em: <http://normas.receita.fazenda.gov.br/sijut2consulta/link.action?visao=anotado&idAto=30552>. Acesso em: 24 fev. 2023.

BRASIL. Secretaria Especial da Receita Federal do Brasil. **Portaria RFB nº 4.820, de 19 de novembro de 2020**. Aprova o Manual Eletrônico do Sigilo Fiscal da Secretaria Especial da Receita Federal do Brasil (e-MSF). Boletim de Serviço da RFB, Brasília, DF, 23 nov. 2020, seção 1, p. 2. Disponível em: <http://normas.receita.fazenda.gov.br/sijut2consulta/link.action?naoPublicado=&idAto=113904&visao=anotado>. Acesso em: 24 fev. 2023.

BRASIL. Supremo Tribunal Federal. **ADI nº 1.480 MC**. Rel. Min. Celso de Mello. Brasília, DF, Plenário, j. 04/09/1997, DJ 18/05/2001. Disponível em: <https://jurisprudencia.stf.jus.br/pages/search/sjur18417/false>. Acesso em: 8 out. 2023.

BRASIL. Supremo Tribunal Federal. **ADI nº 2.859**. Rel. Min. Dias Toffoli. Brasília, DF, Plenário, j. 24/2/2016, DJ 21/10/2016. Disponível em: <https://jurisprudencia.stf.jus.br/pages/search/sjur358417/false>. Acesso em: 6 out. 2023.

BRASIL. Supremo Tribunal Federal. **ADI nº 5.729**. Rel. Min. Roberto Barroso. Brasília, DF, Plenário, j. 8/3/2021, DJ 17/3/2021. Disponível em: <https://jurisprudencia.stf.jus.br/pages/search/sjur442417/false>. Acesso em: 6 out. 2023.

BRASIL. Supremo Tribunal Federal. **ADI nº 6.387 MC-Ref**, Rel. Min. Rosa Weber. Brasília, DF, Plenário, j. 7/5/2020, *DJ* 12/11/2020. Disponível em: <https://jurisprudencia.stf.jus.br/pages/search/sjur436273/false>. Acesso em: 8 out. 2023.

BRASIL. Supremo Tribunal Federal. **ADI nº 6.649**. Rel. Min. Gilmar Mendes. Brasília, DF, Plenário, j. 15/9/2022, *DJ* 19/6/2023. Disponível em: <https://jurisprudencia.stf.jus.br/pages/search/sjur482122/false>. Acesso em: 6 out. 2023.

BRASIL. Supremo Tribunal Federal. **ADPF nº 695**. Rel. Min. Gilmar Mendes. Brasília, DF, Plenário, j. 15/9/2022, *DJ* 19/6/2023. Disponível em: <https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=768683763>. Acesso em: 6 out. 2023.

BRASIL. Supremo Tribunal Federal. **HC nº 91.867/PA**. Rel. Min. Gilmar Mendes. Brasília, DF, Segunda Turma, j. 24/4/2012, *DJ* 20/9/2012. Disponível em: <https://jurisprudencia.stf.jus.br/pages/search/sjur214794/false>. Acesso em: 5 out. 2023.

BRASIL. Supremo Tribunal Federal. **HC nº 124.322 AgR/RS**. Rel. Min. Roberto Barroso. Brasília, DF, Primeira Turma, j. 9/12/2016, *DJ* 19/12/2016. Disponível em: <https://jurisprudencia.stf.jus.br/pages/search/sjur362409/false>. Acesso em: 5 out. 2023.

BRASIL. Supremo Tribunal Federal. **HC nº 168.052/SP**. Rel. Min. Gilmar Mendes, Segunda Turma, j. 20/10/2020, *DJ* 2/12/2020.

BRASIL. Supremo Tribunal Federal. **MS nº 21.729/DF**. Rel. Min. Marco Aurélio, Redator p/ acórdão Min. Néri da Silveira. Brasília, DF, Plenário, j. 5/10/1995, *DJ* 19/10/2001. Disponível em: <https://jurisprudencia.stf.jus.br/pages/search/sjur101299/false>. Acesso em: 5 out. 2023.

BRASIL. Supremo Tribunal Federal. **RE nº 229.096/RS**. Rel. Min. Cármen Lúcia. Brasília, DF, Plenário, j. 16/8/2007, *DJ* 11/4/2008. Disponível em: <https://jurisprudencia.stf.jus.br/pages/search/sjur88728/false>. Acesso em: 8 out. 2023.

BRASIL. Supremo Tribunal Federal. **RE nº 389.808/PR**. Rel. Min. Marco Aurélio. Brasília, DF, Plenário, j. 15/12/2010, *DJ* 10/05/2011. Disponível em: <https://jurisprudencia.stf.jus.br/pages/search/sjur191883/false>. Acesso em: 6 out. 2023.

BRASIL. Supremo Tribunal Federal. **RE nº 418.416/SC**. Rel. Min. Sepúlveda Pertence. Brasília, DF, Plenário, j. 10/5/2006, *DJ* 19/12/2006. Disponível em: <https://jurisprudencia.stf.jus.br/pages/search/sjur92577/false>. Acesso em: 5 out. 2023.

BRASIL. Supremo Tribunal Federal. **RE nº 601.314/SP**. Rel. Min. Edson Fachin, Brasília, DF, Plenário, j. 24/2/2016, *DJ* 16/9/2016. Disponível em:

<https://jurisprudencia.stf.jus.br/pages/search/sjur356216/false>. Acesso em: 6 out. 2023.

BRASIL. Supremo Tribunal Federal. **RE nº 1.027.633/SP**. Rel. Min. Marco Aurélio. Brasília, DF, Plenário, j. 14/8/2019, *DJ* 6/12/2019. Disponível em: <https://jurisprudencia.stf.jus.br/pages/search/sjur416502/false>. Acesso em: 6 out. 2023.

BRASIL. Supremo Tribunal Federal. **RE nº 1.055.941/SP**. Rel. Min. Dias Toffoli. Brasília, DF, Plenário, j. 4/12/2019, *DJ* 18/3/2021. Disponível em: <https://jurisprudencia.stf.jus.br/pages/search/sjur433179/false>. Acesso em: 6 out. 2023.

BRASIL. Supremo Tribunal Federal. **RHC nº 132.062/RS**. Rel. Min. Marco Aurélio. Brasília, DF, Primeira Turma, j. 22/11/2016, *DJ* 24/10/2017. Disponível em: <https://jurisprudencia.stf.jus.br/pages/search/sjur375834/false>. Acesso em: 5 out. 2023.

CASTELLS, Manuel. **The network society: a cross-cultural perspective**. Cheltenham: Edward Elgar Publishing Limited, 2004.

CELESTE, Edoardo. **Digital Constitutionalism: the role of internet bill of rights**. Nova Iorque: Routledge, 2023.

CELLA, José Renato Gaziero; COPETTI, Rafael. Compartilhamento de dados pessoais e a Administração Pública brasileira. **Revista de Direito, Governança e Novas Tecnologias**, Maranhão, v. 3, n. 2, p. 39-58, 2017.

COCKFIELD, Arthur J. Big Data and Tax Haven Secrecy. **Florida Tax Review**, v. 18, p. 483-539, 2016. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2757268. Acesso em: 20 maio 2023.

COCKFIELD, Arthur J. International Tax Transparency. **Perspectives on Tax Law and Policy**, v. 1, n. 4, p. 1-17, dez. 2020. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3753715. Acesso em: 20 maio 2023.

COCKFIELD, Arthur J. Sharing Tax Information in the 21st Century: Big Data Flows and Taxpayers as Data Subjects. **Canadian Tax Journal**, v. 67, n. 4, p. 1179-1199, 2019.

DEAN, Steven A. The incomplete global market for tax information. **Boston College Law Review**, v. 49, n. 605, p. 605-672, 2008. Disponível em: <https://brooklynworks.brooklaw.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1434&context=faculty>. Acesso em: 24 fev. 2023.

DEBELVA, Filip.; MOSQUERA VALDERRAMA, Irma Johanna. Privacy and confidentiality in exchange of information procedures: some uncertainties, many issues, but few solutions. **Intertax**, v. 45, n. 5, p. 362-381, 2017.

ESTADOS UNIDOS. Supreme Court of the United States. **CIC Services, LLC v. Internal Revenue Service, 593 U.S. 19-930 (2021)**. Washington, 2021.

ESTADOS UNIDOS. Supreme Court of the United States. **Olmstead v. United States, 277 U.S. 438 (1928)**. Washington, 1928.

ESTADOS UNIDOS. U.S. Department of the Treasury. **Agreement between the Government of the United States of America and the Government of the Federative Republic of Brazil to Improve International Tax Compliance and to Implement FATCA**. Disponível em: <https://home.treasury.gov/system/files/131/FATCA-Agreement-Brazil-9-23-2014.pdf>. Acesso em: 20 maio 2023.

ESTADOS UNIDOS. United States Court of Appeals For the First Circuit. **James Harper v. Charles P. Rettig, in His Official Capacity as IRS Comm'r, IRS & John Doe IRS Agents 1-10**. Case 21-1316 (2022). Boston, 2022.

FEINER, Lauren. Google and Meta got customer data from tax prep firms, and lawmakers want a probe. **CNBC**. 12 jul. 2023. Disponível em: <https://www.cnbc.com/2023/07/12/google-meta-got-data-from-tax-prep-firms-lawmakers-call-for-probe.html>. Acesso em: 23 jul. 2023.

FERRAZ JÚNIOR, Tércio. Sigilo de dados: o direito à privacidade e os limites da função fiscalizadora do Estado. **Revista da Faculdade de Direito da Universidade de São Paulo**, v. 88, p. 439-459, 1993. Disponível em: <https://www.revistas.usp.br/rfdusp/article/view/67231>. Acesso em: 20 maio 2023.

FETZER, Thomas; YOO, Christopher S. New Technologies and Constitutional Law. **Faculty Scholarship at Penn Law**, n. 545, 2012.

FONSECA, Reynaldo Soares da; FONSECA, Gabriel Campos Soares da; SANTOS, João Gabriel Costa dos. **Jurisdição Constitucional e novas tecnologias: releituras do art. 5º, inciso XII, da Constituição na jurisprudência do Supremo Tribunal Federal**. In: MENDES, Gilmar Ferreira; PIMENTA DE FREITAS, Matheus (Orgs.). **Constituição, Direito Penal e Novas Tecnologias**. São Paulo: Almedina Brasil, 2023.

FRAZÃO, Ana. Propósitos, desafios e parâmetros gerais dos programas de *compliance* e das políticas de proteção de dados. In: FRAZÃO, Ana; CUEVA, Ricardo Villas Bôas (Orgs.). **Compliance e Política de Proteção de Dados**. São Paulo: Thomson Reuters Brasil, 2021. p. 33-62.

HOFFMANN-RIEM, Wolfgang. Innovaciones en la jurisprudencia del Tribunal Constitucional Alemán, a propósito de la garantía de los derechos fundamentales en respuesta a los cambios que conducen a la Sociedad de la Información. **Direito Público**, v. 12, n. 64, p. 40-61, jul./ago. 2015.

JUSTEN FILHO, Marçal. Sistema constitucional tributário: uma aproximação ideológica. **Revista da Faculdade de Direito da UFPR**, Curitiba, a. 30, n. 30, p. 215-233, 1998. Disponível em: <https://revistas.ufpr.br/direito/article/view/1894/1589>. Acesso em: 20 maio 2023.

KEUNEN, Liesa. **The right to privacy used as a modern pillory in L.B. v. Hungary**. Strasbourg Observers, 2021. Disponível em: <https://strasbourgobservers.com/2021/03/01/the-right-to-privacy-used-as-a-modern-pillory-in-l-b-v-hungary/>. Acesso em: 20 jun. 2023

LESSIG, Lawrence. Reading the Constitution in Cyberspace. **Emory Law Journal**, v. 45, n. 3, p. 869-910, 1996.

LIMA, Juciléia. Proteção de Dados dos Contribuintes na Troca de Informações Fiscais. **Revista Direito Tributário Atual**, São Paulo, n. 38, p. 34-52, 2017. Disponível em: <https://revista.ibdt.org.br/index.php/RDTA/article/view/332/649>. Acesso em: 10 maio 2023.

LIOTTI, Belisa Ferreira. Taxpayers' data protection: Do international, regional, and domestic instruments guarantee adequate rights in tax (A)Eol? **Intertax**, v. 50, n. 2, p. 138-158, 2022. DOI: <https://doi.org/10.54648/taxi2022014>. Disponível em: <https://kluwerlawonline.com/journalarticle/Intertax/50.2/TAXI2022014>. Acesso em: 24 fev. 2023.

MARQUES, Thiago de Mattos; LIOTTI, Belisa Ferreira. Troca de informações fiscais e o direito ao sigilo nas perspectivas doméstica e internacional: análise à luz dos requisitos fixados pelo STF nos precedentes de 2016. **Revista Direito Tributário Internacional Atual**, São Paulo, n. 9, ano 5, p. 177-212, 1º sem. 2021.

MENDES, Gilmar Ferreira. Controle de Constitucionalidade: Hermenêutica Constitucional e Revisão de Fatos e Prognoses Legislativos pelo Órgão Judicial. **Revista de Direito Constitucional e Internacional**, v. 8, n. 31, p. 90-108, abr./jun. 2000.

MENDES, Gilmar Ferreira. O direito fundamental à proteção de dados pessoais e a abertura da ordem constitucional à transformação tecnológica: análise do julgamento da ADI 6.387. In: ROCHA, Maria Elizabeth Guimarães Teixeira; BASTOS, Ana Carolina Andrada Arrais Caputo; SILVA, Christine Oliveira Peter da; SILVA, Cristina Maria Gama Neves da; D'ALBUQUERQUE, Julia de Baére Cavalcanti; OLIVEIRA, Manuela Simões Falcão Alvim de (Orgs.). **Ela Pedre Vista**: estudos em homenagem à Ministra Rosa Weber. Londrina: Thoth, 2023. p. 329-348.

MENDES, Gilmar Ferreira; FERNANDES, Victor Oliveira. Constitucionalismo digital e jurisdição constitucional: uma agenda de pesquisa para o caso brasileiro. **Revista Brasileira de Direito**, Passo Fundo, v. 16, n. 1, p. 1-33, jan./abr., 2020.

MENDES, Laura Schertel Ferreira. Autodeterminação informativa: a história de um conceito. **Revista de Ciências Jurídicas Pensar**, Fortaleza, v. 25, n. 4, p. 1-18, out./dez. 2020. Disponível em: <https://ojs.unifor.br/rpen/article/view/10828/pdf>. Acesso em: 20 maio 2023.

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

MÜLLER, Friedrich. **Teoria Estruturante do Direito**. Tradução de Peter Naumann e Eurides Avance de Souza. São Paulo: Revista dos Tribunais, 2008.

MURPHY, Liam; NAGEL, Thomas. **O Mito da propriedade**: os impostos e a justiça. Tradução de Marcelo Brandão Cipolla. São Paulo: Martins Fontes, 2005.

OCDE. **Automatic Exchange of Information**: what it is, how it works, benefits, what remains to be done. Paris: OECD Publishing, 2012. Disponível em: <https://www.oecd.org/ctp/exchange-of-tax-information/automatic-exchange-of-information-report.pdf> . Acesso em: 24 fev. 2023.

OCDE. **Combate à Erosão da Base Tributária e à Transferência de Lucros**. Paris: OECD Publishing, 2013. Disponível em: https://read.oecd-ilibrary.org/taxation/combate-a-erosao-da-base-tributaria-e-a-transferencia-de-lucros-portuguese-version_9789264201248-pt#page1 . Acesso em: 24 fev. 2023.

OCDE. **Recommendation of the Council on Digital Government Strategies**. Paris: OECD Publishing, 2014. Disponível em: <https://www.oecd.org/gov/digital-government/recommendation-on-digital-government-strategies.htm> . Acesso em: 20 maio 2023.

OCDE. **Tax Transparency and Exchange of Information in Times of COVID-19**: 2020 Global Forum Annual Report. Paris: OECD Publishing, 2020. Disponível em: <https://www.oecd.org/tax/transparency/documents/global-forum-annual-report-2020.pdf> . Acesso em: 24 fev. 2023.

OCDE. **The Path to Becoming a Data-Driven Public Sector**. Paris: OECD Publishing, 2019. Disponível em: <https://www.oecd.org/gov/the-path-to-becoming-a-data-driven-public-sector-059814a7-en.htm> . Acesso em: 24 jul. 2023.

OCDE. **Update on Voluntary Disclosure Programmes**: A pathway to tax compliance. Paris: OECD Publishing, 2015. Disponível em: <https://www.oecd.org/ctp/exchange-of-tax-information/update-on-voluntary-disclosure-programmes-a-pathwayto-tax-compliance.htm> . Acesso em: 24 fev. 2023.

ORWELL, George. **1984**. Tradução de Heloisa Jahn e Alexandre Hubner. São Paulo: Companhia das Letras, 2009.

PINHEIRO, Patricia Peck. **Direito Digital**. 7. ed. São Paulo: Saraiva Educação, 2021.

PURPURA, Andrea. Case Law Note: Protection of Taxpayers' Personal Data and National Tax Interest: A Misstep by the European Court of Human Rights? **Intertax**, v. 49, n. 12, p. 1044-1055, 2021.

QUEIROZ E SILVA, Jules Michelet Pereira. **Standards de Prova no Direito Tributário**. São Paulo: IBDT, 2022.

QUEIROZ, Rafael Mafei Rabelo; PONCE, Paula Pedigoni. Tércio Sampaio Ferraz Júnior e Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado: o que permanece e o que deve ser reconsiderado. **Revista Internet & Sociedade**, São Paulo, v. 1, n. 1, p. 64-90, fev. 2020.

RAYPORT, Jeffrey F.; SVIOKLA, John J. Exploiting the Virtual Value Chain. **Harvard Business Review**, nov./dez. 1995. Disponível em: <https://hbr.org/1995/11/exploiting-the-virtual-value-chain>. Acesso em: 24 fev. 2023.

ROCHA, Sergio André. **Troca de Informações para Fins Fiscais**. São Paulo: Quartier Latin, 2015.

RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

RODOTÀ, Stefano. **Tecnologie e diritti**. Bologna: il Mulino, 1995.

RONCO, Stefano Maria. Data Protection in Direct Tax Matters and Developments from the EU Standpoint: The Case of Automatic Exchange of Information. **International Tax Studies (ITAXS)**, v. 3, n. 4, 2020.

SCARCELLA, Luisa. Tax compliance and privacy rights in profiling and automated decision making. **Internet Policy Review**, v. 8, n. 4, p. 2, 2019. Disponível em: <https://policyreview.info/articles/analysis/tax-compliance-and-privacy-rights-profiling-and-automated-decision-making>. Acesso em: 25 jun. 2023.

SCHAPER, Marcel. Data Protection Rights and Tax Information Exchange in the European Union: An Uneasy Combination. **Maastricht Journal of European and Comparative Law**, v. 23, n. 3, p. 514-530, 2016. Disponível em: <https://cris.maastrichtuniversity.nl/en/publications/data-protection-rights-and-tax-information-exchange-in-the-europe>. Acesso em: 24 fev. 2023.

SCHERMER, Bart. Risks of profiling and the limits of data protection law. *In*: CUSTERS, Bart; CALDERS, Toon; SCHERMER, Bart; ZARSKY, Tal (Orgs.). **Discrimination and privacy in the information society**: data mining and profiling in large databases. v. 3. Berlim: Springer, 2013. p. 137-152.

SCHOUERI, Luís Eduardo; BARBOSA, Mateus Calicchio. Da antítese do sigilo à simplicidade do sistema tributário: desafios da transparência fiscal internacional. *In*: SANTI, Eurico Marcos Diniz; CHRISTOPOULOS, Basile Georges; ZUGMAN, Daniel Leib; BASTOS, Frederico Silva (Orgs.). **Transparência Fiscal e desenvolvimento**: homenagem ao Professor Isaías Coelho. São Paulo: FISCOsoft, 2013. p. 497-523.

SCHOUERI, Luís Eduardo; BARBOSA, Mateus Calicchio. Transparency: from tax secrecy to the simplicity and reliability of the tax system. **British Tax Review**, v. 5, p. 666-681, 2013.

SEER, Roman. Proteção de dados e tributação na Alemanha: repercussões do Regulamento Geral sobre Proteção de Dados. Tradução de Diogo Brandau Signoretti. **Revista Jurídica da Presidência**, Brasília, v. 22, n. 126, p. 20-47, fev./maio 2020. Disponível em: <https://revistajuridica.presidencia.gov.br/index.php/saj/article/view/2128/1331>. Acesso em: 20 maio 2023.

SEGUNDO, Hugo de Brito Machado. **Código Tributário Nacional**: anotações à Constituição, ao Código Tributário Nacional e às Leis Complementares 87/1996 e 116/2003. 6. ed., São Paulo: Atlas, 2017.

SILVA, Priscila Stela Mariano da; BOMFIM, Tatiana. **Publicidade on-line sob a perspectiva internacional**: uma análise dos casos Google no mundo. *In*: PISCITELLI, Tathiane (Org.). **Tributação da Economia Digital**. São Paulo: Thomson Reuters Brasil, 2018. p. 127-143.

SOLOVE, Daniel J. **Nothing to hide**: the false tradeoff between privacy and security. New Haven: Yale University Press, 2011.

SOLOVE, Daniel J. **Understanding Privacy**. Cambridge: Harvard University Press, 2008.

SUNSTEIN, Cass R. Constitutional Caution. **University of Chicago Legal Forum**, v. 361, p. 361-375, 1996.

TEDH. **Case of L.B. v. Hungary, app. nº 36345/16**. Fourth Section, j. 12/1/2021. Disponível em: <https://hudoc.echr.coe.int/eng?i=001-207132>. Acesso em: 20 jun. 2023.

TEDH. **Case of L.B. v. Hungary, app. nº 36345/16**. Grand Chamber, j. 9/3/2023. Disponível em: [https://hudoc.echr.coe.int/fre#{%22itemid%22:\[%22001-223675%22\]}](https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-223675%22]}). Acesso em: 20 jun. 2023.

THIMMESCH, Adam B. Transacting in data: tax, privacy, and the new economy. **Denver Law Review**, v. 94, n. 1, p. 145-194, 2016.

UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). **Jornal Oficial da União Europeia**, L 119, p. 1-88, 4 maio 2016. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679>. Acesso em: 20 maio 2023.

VAN OOIJEN, Charlotte; UBALDI, Barbara; WELBY, Benjamin. **A data-driven public sector**: Enabling the strategic use of data for productive, inclusive and trustworthy governance. OECD Working Papers on Public Governance. Paris: OECD Publishing, n. 33, 2019. Disponível em: https://www.oecd-ilibrary.org/governance/a-data-driven-public-sector_09ab162c-en. Acesso em: 24 jul. 2023.

VIOL, Andrea Lemgruber. A Administração Tributária moderna e a maximização do cumprimento tributário: algumas reflexões sobre o caso brasileiro. **Revista da Receita Federal**: estudos tributários e aduaneiros, Brasília, v. 1, n. 2, p. 50-82, jan./jul. 2015. Disponível em: <https://www.gov.br/receitafederal/pt-br/centrais-de-conteudo/publicacoes/revistas/revista-da-receita-federal/2015-revista-de-estudos-tributarios-e-aduaneiros-da-receita-federal-1.pdf/view>. Acesso em: 20 maio 2023.

WARREN, Samuel D.; BRANDEIS, Louis D. The Right to Privacy. **Harvard Law Review**, v. 4, n. 5, p. 193-220, 1890. Disponível em: <https://www.jstor.org/stable/1321160>. Acesso em: 20 maio 2023.

WIMMER, Miriam. Cidadania, tecnologia e governo digital: proteção de dados pessoais no Estado movido a dados. *In*: BARBOSA, Alexandre F. (Org.). **TIC Governo Eletrônico 2019**. Pesquisa sobre o uso das tecnologias de informação e comunicação no setor público brasileiro. 1. ed. São Paulo: Comitê Gestor da Internet no Brasil, 2020.

WIMMER, Miriam. O regime jurídico do tratamento de dados pessoais pelo Poder Público. *In*: DONEDA, Danilo; SARLET, Ingo Wolfgang; MENDES, Laura Schertel; RODRIGUES JUNIOR, Otavio Luiz (Orgs.). **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021. p. 271-288.

WÖHRER, Victoria. **Data Protection and Taxpayers' Rights**: Challenges Created by Automatic Exchange of Information. Amsterdam: IBFD, 2018.

XAVIER, Alberto. Do lançamento: teoria geral do ato, do procedimento e do processo tributário. 2. ed. Rio de Janeiro: Forense, 1998 *apud* QUEIROZ E SILVA, Jules Michelet Pereira. **Standards de Prova no Direito Tributário**. São Paulo: IBDT, 2022.