

DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS PESSOAIS E OS LIMITES DA FISCALIZAÇÃO TRIBUTÁRIA

FUNDAMENTAL RIGHT TO PERSONAL DATA PROTECTION AND THE LIMITS OF TAX SUPERVISION

Alisson Possa¹
Luciano Felício Fuck²

Resumo: A Emenda Constitucional nº 115/2022 estabeleceu como direito fundamental a proteção aos dados pessoais, inclusive nos meios digitais. Acompanhada dos parâmetros da Lei nº 13.709/18, todos os tratamentos de dados pessoais, incluindo os realizados pelo Poder Público, devem observar esse novo contexto normativo, gerando questões acerca de como encontrar um regime de coexistência entre atividades de monitoramento para fins de fiscalização tributária baseadas em dados pessoais e essa nova realidade. O presente artigo desenvolve análise dos reflexos que esse novo quadro normativo impõe aos agentes responsáveis pela fiscalização tributária, principalmente a avaliação dos riscos decorrentes da adoção de sistemas informacionais que realizam análises automatizadas, valendo-se de revisão bibliográfica da doutrina e jurisprudência nacional acerca do conteúdo de direito fundamental da proteção de dados pessoais e os atuais conflitos com os poderes de monitoramento através de bases de dados pessoais pelos agentes de fiscalização tributária, para, então, identificar parâmetros e limites que a proteção de dados pessoais como direito fundamental devem impor aos agentes públicos.

Palavras-chave: proteção de dados; direitos fundamentais; fiscalização tributária; poder público; direito administrativo.

Abstract: The Constitutional Amendment No. 115/2022 established the protection of personal data, including in digital media, as a fundamental right. Accompanied by the parameters of Law No. 13,709/18, all processing of personal data, including those carried out by the Public Authorities, must observe this new normative context, generating questions about how to find a regime of coexistence between monitoring activities for inspection purposes tax based on personal data and this new reality. This article develops an analysis of the consequences that this new regulatory framework imposes on agents responsible for tax inspection, mainly the assessment of risks arising from the adoption of information systems that carry out automated analyses, using a bibliographical review of doctrine and national jurisprudence regarding the content fundamental right to the protection of personal data and the current conflicts with the powers of monitoring through personal databases by tax inspection agents, to then identify parameters and limits that the protection of personal data as a fundamental right must impose on agents public.

Keywords: data protection; fundamental rights; tax fiscalization; public power; administrative law.

Recebido em 17 de fevereiro de 2023

Avaliado em 21 de novembro de 2023 (AVALIADOR A)

Avaliado em 12 de novembro de 2023 (AVALIADOR B)

Aceito em 21 de novembro de 2023

¹ Mestre em Direito Constitucional pelo Instituto Brasileiro de Direito Público; Graduado em Direito pela Universidade Federal de Pelotas. <https://orcid.org/0000-0002-7778-016X>. alisson.possa@gmail.com.

² Doutor em Direito pela Universidade de São Paulo; Mestre em Direito pela Ludwig-Maximilians-Universität. <https://orcid.org/0000-0002-6097-7513>. lucianofelicio@gmail.com.

Introdução

A evolução da tecnologia veio acompanhada de crescimento econômico, novos serviços e produtos para empresas, ferramentas para a melhoria do funcionamento dos Estados e novos tipos de riscos para os cidadãos.

Algoritmos cada vez mais avançados conseguem analisar bases de dados imensas em intervalos de tempos cada vez menores, possibilitando inferências de informações para tomadas de decisões com níveis de probabilidade que praticamente eliminam o risco de erros. Esses algoritmos inauguraram técnicas de análise de dados (*data analytics*), que estão intimamente ligados a um sistema de coleta de grandes bases de dados (*big data*) por empresas de tecnologias.

Os Estados passaram a aplicar essas novas tecnologias para melhorar a sua eficácia por meio da automação de atividades cotidianas ou novas maneiras realização de atividades que são de sua competência.

Dentre essas novas utilizações, o poder de fiscalização tributária passou a contar com ferramentas avançadas para garantir a obrigação tributária dos cidadãos, seja por meio da análise massificada de dados financeiros para melhor calcular o exato montante devido, seja por meio de algoritmos que permitem a indicação de existência de fraudes com elevado grau de exatidão³.

Contrapondo o poder fiscalizatório Estatal, o direito ao sigilo bancário foi, por muito tempo, o principal instrumento de defesa dos contribuintes. Ocorre que nessa nova era de digitalização e análises de dados somente essas ferramentas legais do século XX talvez não sejam suficientes para impedir abusos por parte do Poder Público.

Nesse contexto, a proteção de dados pessoais se insere como um dos principais institutos jurídicos das últimas décadas para tentar garantir direitos individuais.

Em setembro de 2020 a Lei nº 13.709/18 (Lei Geral de Proteção de Dados Pessoais – LGPD) entrou em vigor com disposições sobre todas as atividades que caracterizam tratamentos de dados pessoais (o art. 5º, inciso X, possui 20 verbos que constituem o termo), aplicável tanto para finalidades econômicas quanto para o setor público. Essa legislação inaugura no Brasil o primeiro conjunto de normas e princípios de maneira estruturada, resultado da necessidade do país em estar alinhado aos padrões regulatórios internacionais para manter sua competitividade de mercado⁴.

O Brasil, recentemente, pela decisão do Supremo Tribunal Federal, em sede de Referendoda Medida Cautelar na Ação Direta de Inconstitucionalidade 6.387 (em conjunto com as ADIs nº6388, 6389, 6390 e 6393) no ano de 2020, reconheceu a proteção de dados pessoais como direito protegido pela Constituição Federal de 1988.

³ Aqui valeria fazer referência aos novos sistemas da RFB, a título de exemplo.

⁴ Segundo a United Nations Conference on Trade and Development (UNCTAD), atualmente, de 194 países, 137 possuem legislações sobre o tema. Disponível em <https://unctad.org/page/data-protection-and-privacy-legislation-worldwide>. Acesso em 12 de setembro de 2022.

Posteriormente, no dia 10 de fevereiro de 2022 a Emenda Constitucional 115 foi promulgada, consagrando a proteção de dados pessoais como um direito fundamental no art. 5º, inciso LXXIX, e garantindo a proteção de dados pessoais nos meios digitais.

Certamente, a EC 115/2022 trará reflexos na proteção individual nas mais variadas relações jurídicas, inclusive entre cidadãos e a administração pública. Nesse âmbito, o presente artigo busca responder ao questionamento: a constitucionalização do direito à proteção de dados pessoais demanda uma reavaliação dos limites da fiscalização tributária pelo fisco?

Para responder o questionamento, o artigo está apoiado na metodologia de revisão bibliográfica que tem como objeto doutrina nacional e jurisprudência do Supremo Tribunal Federal sobre proteção de dados e o atual regime de poderes para fiscalização tributária de agentes públicos.

Para isso, a primeira parte irá esboçar a atual relação de poderes fiscalizatórios que a administração fiscal brasileira possui frente aos limites encontrados pelos direitos dos contribuintes, por meio de uma análise legal e jurisprudencial.

Em seguida, será analisado o processo de constitucionalização da proteção de dados no cenário internacional e nacional.

Por fim, serão expostos os tipos de parâmetros e limites que a proteção de dados pessoais como direito fundamental devem impor aos agentes públicos, e se tais limitações demandam novas avaliações do atual poder fiscalizatório da administração tributária brasileira.

1 Os poderes de fiscalização tributária no Brasil e seus limites

O relevante papel constitucional de estabelecer competências implica possibilitar a materialização dos poderes estatais e o cumprimento de seus deveres e objetivos (Hesse, 1999, p. 12). Assim, a previsão de competências tributárias na Carta Magna significa não só a autorização de instituir tributos, como também de dar os meios para cobrar, apurar e fiscalizar esses tributos⁵.

Por sua vez, a fiscalização está relacionada à noção de conhecimento, no qual o ente estatal busca conhecer informações sobre atividades de seus cidadãos.

Quando abordamos a ideia de conhecimento, estamos falando de poder, segundo a autora Carissa Véliz “conhecimento é poder”⁶, pois *“The more someone knows about us, the more they can anticipate our every move, as well as influence us”* (Véliz, 2021)

Nesse sentido, os poderes de fiscalização tributária garantem ao Estado conhecer o cotidiano dos cidadãos por meio da origem de seus rendimentos, assim como perfis de consumo, relações familiares, evolução profissional etc.

⁵ A propósito da relação entre competência tributária na CF/1988 e direitos fundamentais, cf. Fuck, 2017, p. 63-90.

⁶ Artigo publicado pela autora Carissa Véliz na página Boston Review, intitulado “Why Democracy Needs Privacy” em abril de 2021. Disponível em <https://bostonreview.net/articles/why-democracy-needs-privacy/>.

Importante destacar que a LGPD e o novo direito fundamental à proteção de dados são aplicados somente à dados pessoais, que são aqueles referentes a pessoas naturais (art. 5º, inciso I da LGPD)⁷, e não a dados corporativos relacionados a pessoas jurídicas. Por esse motivo, as regras abaixo citadas são aquelas que garantem à administração pública poder fiscalizatório para verificação de cumprimento das obrigações fiscais por parte de pessoas naturais somente.

Esse poder fiscalizatório consiste na atividade de vigilância que o poder estatal pode exercer sobre os particulares para identificar se as obrigações tributárias foram cumpridas (Janini; Pulcinelli, 2016, p. 349). Sua origem constitucional remonta ao art. 145, §1º da carta de 1988, uma vez que determina a individualização da cobrança de impostos⁸, gerando a necessidade de a Administração verificar os elementos individuais para a correta cobrança (Maldonado, 2020, p. 265).

No âmbito infraconstitucional, o Código Tributário Nacional (CTN) estabelece, no art. 194 e seguintes um capítulo sobre poderes dos entes fiscalizatórios em requerer informações para várias fontes a fim de identificar bens, negócios ou atividades de terceiros (pessoas físicas ou jurídicas) para verificar o cumprimento das obrigações tributárias.

Importante ressaltar que a proteção de dados pessoais tem como o todos os dados que identificam diretamente ou permitem a identificação da pessoa natural a que se refere⁹. Portanto, alguns dados relativos a pessoas jurídicas, como aqueles relativos aos balanços financeiros, não entram nesse escopo de proteção, motivo pelo qual toda a análise aqui exposta será referente à sistemas e normas que têm como objeto dados referentes a pessoas naturais.

O art. 197 do CTN possibilita o requerimento de dados e informações de terceiros àqueles indicados nos seus incisos, gerando o poder do Estado em obter dados pessoais de titulares que foram coletados por terceiros. Ainda, o art. 200 do CTN estabelece a possibilidade de as autoridades administrativas se valerem das forças públicas em nível federal, estadual ou municipal para efetivar as medidas fiscalizatórias.

Em âmbito federal, o Decreto nº 3.724/01, que regulamenta o art. 6º da Lei Complementar 105, estabelece, em seu art. 3º, a possibilidade da Receita Federal do Brasil (RFB) obter dados e informações de instituições financeiras, sejam eles sobre pessoas jurídicas ou físicas. Mais sobre essa questão na análise sobre o sigilo bancário abaixo.

Ainda, o Conselho Administrativo de Recursos Fiscais – CAREF, reconhece amplo poder de fiscalização de livros e documentos previstos no art. 195 que suportem a incidência tributária,

⁷ Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

⁸ § 1º Sempre que possível, os impostos terão caráter pessoal e serão graduados segundo a capacidade econômica do contribuinte, facultado à administração tributária, especialmente para conferir efetividade a esses objetivos, identificar, respeitados os direitos individuais e nos termos da lei, o patrimônio, os rendimentos e as atividades econômicas do contribuinte.

⁹ Esse conceito está previsto no art. 5º, inciso I da LGPD: dado pessoal: informação relacionada a pessoa natural identificada ou identificável.

assim como a exigência de um dever de apresentação dos documentos exigidos para o contribuinte (Maldonado, 2020, p. 280). A natureza da atividade de fiscalização tributária do Estado é vista como uma atividade administrativa e deve observar os ditames do direito administrativo. Segundo Janini e Pulcinelli (2016, p. 350)

Parece não haver dúvidas de que a atividade de fiscalização tributária caracteriza-se como um ato da Administração Pública, sujeitando-se, portanto, ao regime jurídico administrativo, ou seja, ao conjunto de regras e princípios que outorgam identidade ao direito administrativo em face do direito privado, caracterizado pelo binômio prerrogativas/restrições. Atualmente, é importante consignar, que os princípios ganham papel de relevo na normatização das relações jurídicas, especialmente as de direito público.

Dentro das limitações relativas à natureza da atividade administrativa, é evidenciado o princípio da legalidade (Janini; Pulcinelli, 2016, p. 352). Esse princípio é entendido como um mecanismo de defesa do contribuinte pois todos os atos relativos à atividade de fiscalização devem observar a necessidade de ato legal com os parâmetros necessários à sua realização.

Já a segunda limitação está na ordem dos direitos individuais dos contribuintes, sendo o sigilo bancário o principal, cuja previsão decorre de uma interpretação dos incisos X e XII do art. 5º da Constituição Federal, que tratam sobre a inviolabilidade da intimidade das correspondências e dados.

A Lei Complementar 105/01 estabeleceu parâmetros para o sigilo das operações de instituições financeiras, abrangendo os dados bancários dos cidadãos.

Até o julgamento do Recurso Extraordinário nº 601.314 era entendido que a quebra do sigilo bancário só podia ocorrer mediante ordem judicial em situações que fossem verificados indícios de “sonegação, lavagem de dinheiro, peculato, concussão, corrupção ativa ou passiva, excesso de exação, negociações que impliquem abuso de poder econômico” (Martins, 2011, p. 96).

O julgamento, que questionava a permissão de acesso dos entes de fiscalização tributária a dados bancários dos contribuintes frente previsto no art. 6º da Lei Complementar 105/01, acabou por criar uma flexibilização nesse direito individual. Nesse sentido, o Ministro Fachin se manifestou:

Nesses termos, a identificação do patrimônio, rendimentos e atividades econômicas do contribuinte pela Administração Tributária serve para a efetivação do princípio da capacidade contributiva, o qual, por sua vez, encontra-se em risco de violação em todas as restritivas hipóteses autorizadoras de acesso da Administração Tributária às transações bancárias dos contribuintes, tal como arroladas nos incisos do art. 3º do Decreto 3.724/01, que regulamenta o art. 6º da lei impugnada (Brasil, 2020, p. 20).

O entendimento foi de que o sigilo bancário poderia ser afastado mediante mero processo administrativo para acesso de dados referentes a contas de depósito e aplicações financeiras quando necessários pelos entes fiscalizadores, uma vez que, de outra maneira, estaria em risco a efetivação do princípio da capacidade contributiva.

2 A constitucionalização da proteção de dados pessoais

A proteção de dados pessoais é uma nova manifestação do direito à privacidade, um direito fundamental que garante aos indivíduos seu livre desenvolvimento.

O início da proteção à privacidade como direito fundamental é remetido ao clássico artigo *The right to privacy*, de Brandeis e Warren (1890).

Essa primeira versão do direito à privacidade tinha como característica uma individualidade extrema (Doneda, 2019, p. 30). Ainda que com o tempo essa conceituação tenha sofrido mudanças, principalmente por conta de mudanças econômicas e sociais, o elemento da privacidade como um direito individual que garante proteção de uma esferada vida humana contra invasões indesejáveis permanece.

Esse mesmo elemento ganha contornos importantes na sociedade informacional em que muitas das ameaças às várias dimensões da privacidade não são originadas só pelo Estado, mas também por empresas que passam a rivalizar o poder estatal em muitos aspectos de controle e regulação social.

É nesse sentido que a proteção de dados surge como uma nova manifestação do direito à privacidade no contexto de novas tecnologias de processamento de dados, que inauguram novas ameaças a direitos e liberdades.

As primeiras legislações de proteção de dados surgiram na década de 70, como as Leis do Estado Alemão de Hesse (1970), Lei de dados da Suécia (1973), Lei Federal de Proteção de Dados da Alemanha (1977). Na década seguinte, a Convenção 108 do Conselho da Europa (1981), Diretrizes da OCDE para a proteção de privacidade e dos fluxos fronteiriços de dados pessoais (1980) e a Diretiva Europeia 95/46/CE (1995) acabaram por internacionalizar o tema (Mendes, 2014, p. 30).

Dentre esses instrumentos legais, destacam-se previsões em comum que são sintetizadas em princípios que passaram a acompanhar todo o conteúdo de um direito fundamental à proteção de dados pessoais: (i) transparência sobre a existência de bancos de dados; (ii) exatidão dos dados pessoais armazenados, retratando a realidade; (iii) finalidade pré-definida dos tratamentos, que deve ser informada antes da coleta; (iv) livre acesso dos titulares aos bancos de dados pessoais onde seus dados estão armazenados e (v) segurança física e lógica contra ações que atentem à confidencialidade, integridade ou disponibilidade dos dados pessoais (Doneda, 2011, p. 100-101).

Nesse trajeto legislativo, o Tribunal Constitucional Alemão decidiu, em 1983, sobre um direito fundamental à autodeterminação informativa visando proteger os dados pessoais contra ameaças do Estado por processamentos não transparentes dos dados (BVerfGE 65,1). Esse direito fundamental decorre do direito ao livre desenvolvimento da personalidade e do direito à dignidade humana quando dos riscos que passam a existir com o processamento automatizado de dados pessoais pelo Estado.

Também, no mesmo sentido do reconhecimento em âmbito internacional, a Carta dos Direitos Fundamentais da União Europeia¹⁰ reconhece a proteção de dados pessoais como um direito fundamental no art. 8º. Considerando que o bloco é composto por diversos países, o reconhecimento é importante no sentido de internacionalizar a questão.

Dois casos sobre proteção de dados e fiscalização tributária chamam atenção na União Europeia: o Caso C-175/20 da Corte de Justiça da União Europeia e a imposição de multa ao órgão de fiscalização tributária da Holanda pela Autoridade Holandesa de Proteção de Dados.

O primeiro, Caso C-175/20, estabelece os limites da atividade fiscalizatória perante o direito fundamental à proteção de dados pessoais, e é objeto de análise aprofundada no próximo item.

O segundo caso é referente à decisão da Autoridade Holandesa de Proteção de Dados (Autoriteit Persoonsgegevens) que multou em 3.7 milhões de euros (a maior multa já aplicada pelo órgão) a autoridade administrativa de fiscalização tributária por várias infrações ao Regulamento Geral de Proteção de Dados¹¹.

A sanção foi motivada por um sistema de combate a fraudes (FSV) que funcionou até 2020 e possuía vários problemas de conformidade legal. As inconformidades identificadas foram: discriminação por dados relativos à nacionalidade e aparência física, falta de base legal para o tratamento dos dados, falta de transparência prévia quanto às finalidades do sistema, utilização de dados pessoais incorretos e/ou obsoletos, armazenamento por tempo maior que o necessário, falta de proteção às bases de dados e a sua omissão em realizar medidas para a determinação de riscos do uso do sistema ao setor competente.

São mais de 50 anos de desenvolvimentos interpretativos, culturais e empíricos sobre os institutos e conceitos de proteção de dados pessoais no mundo que o Brasil não acompanhou.

Nacionalmente, esse tema foi tratado de maneira setorial e com pouca profundidade até o advento da Lei Geral de Proteção de Dados (Lei nº 13.709/18). Laura Mendes (2014) cita os seguintes dispositivos com menção à proteção de dados: Código de Defesa do Consumidor (Lei nº 8.078/90), Código Civil (Lei nº 10.406/02), Lei do Cadastro Positivo (Lei nº 12.414/11), decreto do Serviço de Atendimento ao Consumidor (Decreto nº 6.523/08), decreto para cadastro único de programas sociais do Governo Federal (Decreto nº 6.135/07) e decreto do Censo Anual da Educação (Decreto nº 6.425/08).

Esse cenário passa a mudar em 2018 com a aprovação da Lei nº 13.709, a Lei Geral de Proteção de Dados Pessoais, a primeira legislação com regras abrangentes sobre o tema, que

¹⁰ 1. Todas as pessoas têm direito à proteção dos dados de carácter pessoal que lhes digam respeito. 2. Esses dados devem ser objecto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respectiva retificação.

¹¹ O comunicado da decisão pode ser encontrado em inglês no site oficial da Autoridade: <https://autoriteitpersoonsgegevens.nl/en/news/tax-administration-fined-fraud-blacklist>.

estabeleceu, também, princípios. Esses princípios foram reconhecidos como desdobramentos da esfera subjetiva do direito fundamental à autodeterminação informativa pelo Supremo Tribunal Federal.

Em 2020 o tema chegou à Corte Suprema com as ADIs já citadas anteriormente. Elas questionavam uma Medida Provisória que demandava o compartilhamento de dados pessoais dos cidadãos brasileiros sob a guarda das empresas de telecomunicação ao IBGE para a realização do Censo.

O STF decidiu que a Medida era inconstitucional frente ao direito fundamental à proteção de dados baseado em um fundamento de autodeterminação informacional que se depreende do texto constitucional.

A partir deste marco, fica claro que a intervenção do Estado na esfera privada dos cidadãos, através de tratamentos de dados pessoais, passa a encarar um novo cenário constitucional.

Seguindo a decisão do STF, em fevereiro de 2022 foi promulgada a Emenda Constitucional nº 115/22 já citada, que, além de constar o direito à proteção de dados pessoais como direito fundamental na Constituição, também estabeleceu que é competência privativa da União legislar sobre o tema através do inciso XXX do art. 22. Essa reserva de competência é importância no contexto da fiscalização tributária pois retira das secretarias estaduais a possibilidade de criarem regulamentações que flexibilizem esse direito fundamental para a utilização de novas tecnologias.

3 As consequências da constitucionalização da proteção de dados pessoais para a fiscalização tributária

O avanço tecnológico permitiu aos órgãos de fiscalização tributária o emprego de novas ferramentas, não só para a automação de procedimentos, mas também inaugurando possibilidades de inferências sobre informações dos contribuintes.

Como exemplo, a Receita Federal do Brasil, já em 2008, anunciou uma colaboração com a Universidade Estadual de Campinas (Unicamp) e Instituto Tecnológico de Aeronáutica (ITA) o desenvolvimento de algoritmos de inteligência artificial para combater sonegação fiscal¹².

Também, os entes fiscalizadores passaram a contar cada vez mais com diferentes tipos de grandes bases de dados, a exemplo do Protocolo 01/04 estabelecido entre o Secretário da Receita Federal, secretários das fazendas estaduais e do distrito federal e representantes das secretarias de finanças das capitais no I Encontro Nacional de Administradores Tributários (ENAT), criando o Cadastro Sincronizado dos contribuintes (Jarude, 2020)

¹² Disponível em <https://www.serpro.gov.br/menu/noticias/noticias-antigas/receita-federal-implanta-com-apoio-do-serpro-primeiros-modulos-do-software-de-inteligencia-artificial>.

Essas tecnologias ajudam os agentes fiscalizadores a, principalmente, selecionar os contribuintes que serão fiscalizados detalhadamente, uma vez que os cruzamentos de dados e análises algorítmicas permitem indicar inconsistências que podem ser originadas em fraudes, omissões etc.

Por outro lado, as novas ferramentas digitais inauguram novos riscos aos cidadãos, uma vez que não há somente cruzamentos de bases de diferentes categorias de dados, mas, também, há a capacidade de processamento dessas bases em grande escala e com algoritmos personalizados, seja para auxiliar na tomada de decisões seja para gerar informações sobre os titulares.

Ocorre que a atividade de fiscalização tributária acaba por ter acesso à bases com os mais diversos tipos e categorias de dados pessoais, os quais, quando submetidos à algoritmos, podem revelar mais que somente informações fiscais, mas também outras de ordem pessoal. Essas novas informações, por sua vez, podem acabar sendo de grande utilidade não só para a fiscalização do cumprimento de obrigações, mas também para o monitoramento dos cidadãos por parte do Estado.

Como atividade de monitoramento baseada em dados pessoais, é necessário que o órgão público responsável observe os ditames constitucionais e administrativos, principalmente frente às limitações que decorrem do direito fundamental à proteção de dados.

Nesse sentido, reforçando a preocupação com o monitoramento individual, a União Europeia possui um projeto de legislação¹³ sobre os usos de inteligência artificial que classifica algoritmos usados por órgãos da administração da justiça e processos democráticos como de risco elevado no Considerando 40¹⁴.

Pode-se entender que as atividades de fiscalização da Administração Fiscal, que demandam interpretação de determinados fatos para verificação da incidência de tributos ou de ilícitos fiscais, também estão sujeitos aos riscos acima descritos.

Tais riscos, ainda que na ordem de coleta e tratamento algorítmico, dizem respeito a dados pessoais, motivo pelo qual a constitucionalização da proteção de dados tem necessariamente reflexos para o entendimento brasileiro sobre os poderes da fiscalização tributária.

Primeiramente, é oportuno aprofundar sobre a relação entre esse direito fundamental e a atividade de fiscalização tributária realizada pelo Estado. A Corte de Justiça da União Europeia já se manifestou sobre como se dá essa relação, conforme já citado anteriormente.

O Caso C-175/20 diz respeito à um requerimento de dados pessoais da Autoridade Tributária da Letônia à um provedor de serviços de propaganda na internet (SS). A Autoridade

¹³ Disponível em <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:52021PC0206&from=EN>. Acesso em 26 de abril de 2022.

¹⁴ Determinados sistemas de IA concebidos para a administração da justiça e os processos democráticos devem ser classificados como de risco elevado, tendo em conta o seu impacto potencialmente significativo na democracia, no Estado de direito e nas liberdades individuais, bem como no direito à ação e a um tribunal imparcial. Em particular, para fazer face aos riscos de potenciais enviesamentos, erros e opacidade, é apropriado classificar como de risco elevado os sistemas de IA concebidos para auxiliar as autoridades judiciárias na investigação e na interpretação de factos e do direito e na aplicação da lei a um conjunto específico de factos. Contudo, essa classificação não deve ser alargada aos sistemas de IA concebidos para atividades administrativas puramente auxiliares que não afetam a administração efetiva da justiça em casos individuais, como a anonimização ou a pseudonimização de decisões.

solicitando que a empresa permitisse o acesso à Autoridade aos números de chassi dos veículos anunciados no portal da internet da empresa, assim como aos números de telefone dos vendedores.

O requerimento demandava: endereço eletrônico do anúncio, o texto do mesmo, a marca, o modelo, o número de chassis e o preço do veículo, bem como o número de telefone do vendedor, deviam ser apresentadas por via eletrônica em formato que permitisse a filtragem ou a seleção dos dados.

A empresa negou o compartilhamento dos dados pessoais e o caso chegou à Corte de Justiça da União Europeia com questionamentos acerca do alcance de disposições da GDPR às autoridades de fiscalização tributária.

Foi conclusão da Corte que os requerimentos da Autoridade da Letônia atraem a aplicação da GDPR, em especial a necessidade de observar os princípios de proteção de dados (Luxemburgo, 2022, parágrafo 46).

Outro ponto importante da decisão foram as conclusões acerca dos requisitos de atos fiscalizatórios que realizam tratamento de dados pessoais. Em um primeiro requisito, o órgão estabelece a limitação da finalidade, afastando a hipótese de fundamentos abstratos e genéricos:

Daqui resulta que, num caso em que a comunicação dos dados pessoais em causa não se baseia diretamente na disposição legal que constitui o seu fundamento, mas resulta de um pedido da autoridade pública competente, é necessário que esse pedido especifique quais são as finalidades específicas dessa recolha de dados à luz das funções de interesse público ou do exercício da autoridade pública, a fim de permitir ao destinatário do referido pedido assegurar-se de que a transmissão dos dados pessoais em causa é lícita e aos órgãos jurisdicionais nacionais efetuar uma fiscalização da legalidade dos tratamentos em causa (Luxemburgo, 2022, parágrafo 71).

O segundo requisito diz respeito à necessidade dos dados pessoais, que devem estar estritamente ligados à finalidade estrita:

Daqui resulta que o responsável pelo tratamento, incluindo quando atua no âmbito das funções de interesse público de que foi investido, não pode proceder, de forma generalizada e indiferenciada, à recolha de dados pessoais e deve abster-se de recolher dados que não são estritamente necessários à luz das finalidades do tratamento (Luxemburgo, 2022, parágrafo 74).

O terceiro requisito diz respeito à limitação temporal do tratamento somente para alcançar a finalidade estrita:

No que respeita à circunstância de o pedido de comunicação apresentado pela Autoridade Tributária letã não prever, na hipótese de o prestador de serviços de anúncios em causa não ter procedido ao restabelecimento do acesso aos anúncios publicados no período especificado no pedido, nenhum limite temporal, há que recordar que, tendo em conta o princípio da minimização dos dados, o responsável pelo tratamento está igualmente obrigado a limitar ao estritamente necessário, à

luz do objetivo do tratamento previsto, o período de recolha dos dados pessoais em causa. Por conseguinte, o período sobre o qual incide a recolha não pode exceder a duração estritamente necessária para alcançar o objetivo de interesse geral visado (Luxemburgo, 2022, parágrafos 79-80).

Por fim, o quarto requisito é o de um instrumento normativo específico para o tratamento, uma vez que se trata de órgão público:

(...) regulamentação que serve de base ao tratamento deve prever regras claras e precisas que regulem o âmbito e a aplicação da medida em causa e impor requisitos mínimos, de modo que as pessoas cujos dados foram conservados disponham de garantias suficientes que permitam proteger eficazmente esses dados pessoais contra os riscos de abuso. Esta regulamentação deve ser vinculativa no direito interno e, particularmente, indicar em que circunstâncias e em que condições uma medida que prevê o tratamento de tais dados pode ser adotada, garantindo assim que a ingerência seja limitada ao estritamente necessário (...). Daqui resulta que a regulamentação nacional que regula um pedido de comunicação como o que está em causa no processo principal deve basear-se em critérios objetivos para definir as circunstâncias e as condições em que um prestador de serviços em linha está obrigado a transmitir dados pessoais relativos aos seus utilizadores (Luxemburgo, 2022, parágrafos 84-85).

O conteúdo desse julgamento elucida como um órgão público que realiza atividade de interesse público na forma de fiscalização da correta cobrança de tributos, principalmente para garantir a igualdade de cobrança entre os contribuintes, pode conciliar sua função perante o direito fundamental em questão na forma da observância dos princípios que compõem a proteção de dados pessoais.

Esse entendimento também encontra respaldo no Brasil, uma vez que os dois casos relativos à proteção de dados pessoais que foram objeto de julgamento pelo Supremo Tribunal Federal dizem respeito a tratamentos realizados por órgãos públicos. Ainda que não sejam no contexto da fiscalização tributária, o resultado também se aplica aos órgãos competentes.

Uma das consequências desses julgamentos é o surgimento de novos requisitos para a observância do princípio da legalidade, ponto que foi abordado tanto na decisão de 2020 do STF quanto no julgamento contido na ADI 6649 e da ADFP 695, que também questionavam atos do poder público voltados à tratamentos de dados pessoais.

No julgamento de 2020, alguns ministros apontaram que a Medida Provisória questionada não continha informações necessárias, como, por exemplo medidas relativas à segurança (Brasil, 2020, p. 23, 44 e 62), delimitação da finalidade (Brasil, 2020, p. 62 e 107), para sua conformidade a esse direito fundamental. O Ministro Gilmar Mendes, destaca:

A doutrina e a própria legislação aplicável impõem que a autodeterminação só possa ser afastada por um dever de justificação minudente e exaustivo das finalidades atribuídas ao tratamento de dados. No caso em tela, há uma enorme dificuldade de se extrair do texto normativo um contorno mínimo de segurança

sobre a finalidade do tratamento de dados que é simplesmente referenciado com o objetivo de “produção estatística oficial” (Brasil, 2020, p. 111).

Ele também destacou a insuficiência da MP ao justificar a finalidade do tratamento em sucinta expressão de “produção estatística oficial”, além de não observar a transparência, uma vez que não foram informados mecanismos de controle aos titulares (Brasil, 2020, p. 111). Em outro ponto, o ministro também menciona a falta de observância do princípio da adequação, pois não é indicada a efetiva utilidade dos dados coletados para a finalidade pretendida, além de constatar que o princípio da necessidade não foi observado pois outros mecanismos com utilização de menor quantidade de dados poderia ser utilizado (Brasil, 2020, p.113).

O Ministro Roberto Barroso analisa que a constitucionalidade da medida provisória só seria alcançada com previsão específica sobre a limitação da finalidade do tratamento e medidas de segurança adequadas ao escopo do tratamento (Brasil, 2020, p. 44).

O Ministro Luiz Fux lista violações da MP perante princípios que compõem o direito fundamental à proteção de dados. Fora eles: a finalidade, uma vez que a MP não esgotava as finalidades para quais os dados seriam utilizados; a necessidade, pois evidenciada a desproporcionalidade da quantidade de dados coletados em relação à finalidade almejada (pesquisa por amostragem) e segurança, pois inexistente especificação de medidas técnicas suficientes a assegurar a confidencialidade, integridade e disponibilidade dos dados pessoais (Brasil, 2020, p. 62-64).

É possível concluir que o conteúdo de matriz constitucional da proteção de dados, que deve estar expresso em todos os tratamentos de dados pessoais, até mesmo naqueles empregados pelo poder público nas situações em que a LGPD não se aplica (art. 4º), é o dos princípios. Os votos da Suprema Corte já indicam parâmetros interpretativos para o conteúdo de alguns deles e que podem ser utilizados na análise do presente artigo.

Por sua vez, no julgamento ocorrido em 2022 que questionava a constitucionalidade do Decreto nº 10.046/19, conhecido como Decreto Base do Cidadão, também foi objeto de análise a utilização de bases de dados de cidadãos para que atingir finalidades públicas. O Ministro Gilmar Mendes¹⁵ alerta para a necessidade de que a privacidade e a proteção de dados nunca podem ser tratadas como interesses individuais perante tratamentos do poder público, sob pena de que esses direitos fundamentais sempre venham a sucumbir perante o argumento do interesse público (Brasil, 2022, p. 33).

Nesse julgamento também foi constada a responsabilidade do Estado quando comprovados danos causados pelo órgão público responsável pelo tratamento, resguardando o direito de regresso ao próprio agente público responsável:

¹⁵ No presente momento o voto não foi disponibilizado oficialmente pelo Supremo Tribunal Federal, podendo ser encontrado online. Disponível em <https://images.jota.info/wp-content/uploads/2022/09/voto-adi-6649-e-adpf-695-1.pdf> . Acesso em 19 de setembro de 2022.

Assim sendo, o tratamento de dados pessoais promovido por órgãos públicos ao arrepio dos parâmetros legais e constitucionais (ingerência) importará a responsabilidade civil do Estado pelos danos suportados pelos particulares, na forma dos arts. 42 e seguintes da Lei 13.709/2018, associada ao exercício do direito de regresso contra os servidores e agentes políticos responsáveis pelo ato ilícito, em caso de dolo ou culpa (Brasil, 2022, p. 98-99).

Considerando que a adoção de sistemas automatizados para a tomada de decisões no contexto da fiscalização tributária passa por decisões de agentes públicos, o ponto acima destacado pelo Ministro Gilmar Mendes pode vir a se concretizar quando em danos oriundos dessas atividades pelo Estado.

Estabelecidas as limitações que competem ao poder público por conta da sua atividade, serão analisados aqueles limites relativos à direitos fundamentais, em que a proteção dedados pode ser adicionada junto ao sigilo bancário.

Enquanto o sigilo bancário pode ser considerado um direito fundamental no sentido que o Estado deve se abster de acessar informações e dados constantes nas bases de instituições financeiras, esse direito sofreu uma fragilização com a Lei Complementar 105/01: a necessidade de uma decisão judicial passou para a necessidade de um ato administrativo, que pode ser emitido pelo próprio órgão fiscalizador.

De outra seara, o direito fundamental à proteção de dados pessoais possui um duplo âmbito de proteção: proteção do indivíduo contra ameaças à sua personalidade em face do tratamento de dados e garantia de controles de fluxos de dados na sociedade (Mendes, 2014, p. 176). A professora Laura Mendes também destaca que na dimensão subjetiva ele é um direito de defesa, garantindo ao indivíduo a cessão da intervenção, assim como ferramentas para que danos oriundos dessas intervenções sejam evitados ou então indenizado (Mendes, 2014, p. 177).

Na dimensão objetiva do direito fundamental, identifica-se a obrigação do Estado em criar regulações procedimentais para sua garantia, podendo ser entendido, aqui, a previsão de mecanismos procedimentais, como aqueles relativos aos direitos dos titulares naqueles atos do poder público que realizam intervenções na esfera da proteção de dados (Mendes, 2014). São elementos necessários dos mecanismos procedimentais: aqueles para a observância do princípio da transparência sobre o tratamento; a autodeterminação por meio de direitos dos titulares (como direito de acesso, retificação e eliminação); a observância do contexto por meio do princípio da finalidade e adequação; os relativos aos princípio da segurança, através de mecanismos contra a quebra de confidencialidade, integridade e disponibilidade e aqueles relativos à limitação de armazenamento para observância do princípio do esquecimento. Acentuam-se os mecanismos de limitação de tratamento de dados pessoais sensíveis para a observância do princípio da não-discriminação (Mendes, 2014, p. 180).

No caso das ferramentas tecnológicas atualmente empregadas pelas autoridades fiscais, esses direitos também devem sofrer modificações relativas ao tipo de utilização dos dados,

principalmente a elaboração de perfis (técnica conhecida como *profiling*) e tomada de decisões automatizadas (Scarcella, 2019, p. 5).

No primeiro caso, o direito do livre acesso deve não só ser restringido aos dados pessoais efetivamente utilizados, mas também as conclusões que levam à categorização como um determinado tipo de perfil criado previamente.

Também podemos citar a imposição de não-discriminação (art. 6º, inciso IX), que, em técnicas de *profiling* podem acabar por criar e categorizar perfis com critérios discriminatórios. Segundo Wolfgang Hoffman-Riem

De acordo com o Art. 4, N. 4, do Regulamento Básico de Protecção de Dados da UE, o perfil refere-se a “qualquer tratamento automatizado de dados pessoais que consista em utilizar dados pessoais para avaliar certos aspectos pessoais relativos a uma pessoa singular, em particular com vista a analisar ou prever aspectos relativos ao desempenho do trabalho, situação econômica, saúde, preferências pessoais, interesses, confiabilidade, conduta, localização ou deslocamento dessa pessoa singular”. Para criar um perfil, são utilizados algoritmos para avaliar especificamente informações sobre comportamentos anteriores (Hoffman-Riem, 2020, p. 128).

Já no segundo caso, diz respeito ao direito de não ser sujeito a decisões automatizadas, que no Brasil foi incorporado pela LGPD no art. 20 como um direito à revisão de decisões tomadas unicamente em tratamento automatizado.

No contexto da fiscalização tributária os algoritmos utilizados podem acabar, por exemplo, por determinar que a declaração do imposto de renda de determinados indivíduos seja automaticamente marcada para a chamada Malha Fiscal. A Receita Federal explica o procedimento¹⁶:

Quando você envia a sua Declaração de Imposto de Renda, **ela passa por uma análise dos sistemas** da Receita Federal, onde são verificadas as informações que você enviou e elas são comparadas com informações fornecidas por outras entidades (terceiros), que também tem que prestar informações à Receita: empresas, instituições financeiras, planos de saúde e outros. Se for encontrada alguma diferença entre as informações apresentadas por você em relação às informações apresentadas por terceiros, a sua declaração será separada para uma análise mais profunda, é o que se chama de Malha Fiscal (ou “malha fina” como é popularmente conhecida (grifo nosso)).

O órgão explicitamente informa que um sistema realiza a análise e realiza a separação. Nesse caso, o titular pode, com base no art. 20 da LGPD, requerer a revisão dessa decisão junto com a identificação dos critérios que a suportam.

Nesse sentido, é importante que esse direito demanda, necessariamente, que a transparência sobre elementos do tratamento seja suficiente para garantir ao titular informações suficientes para

¹⁶ Disponível em <https://www.gov.br/receitafederal/pt-br/assuntos/meu-imposto-de-renda/malha-fiscal>. Acesso em 26 de abril de 2022.

fundamentar um possível pedido de revisão, como: a informação de dados pessoais tratados, a origem da coleta desses dados e uma explanação com detalhamento razoável sobre os critérios e procedimentos adotados (Possa; Ramos, 2022)

Outro campo em que a Receita Federal emprega sistemas de inteligência artificial é para o controle aduaneiro, como, por exemplo, o Sistema de Seleção Aduaneira por Aprendizagem de Máquina (SISAM), que busca reduzir a evasão fiscal na importação através de cálculos de probabilidade (Jambeiro Filho, 2019, p.12) e que, junto com outros sistemas que unificam bases de dados, pode acabar utilizando dados pessoais de sócios de empresas ou até mesmo colaboradores do setor empresarial.

Nesse caso, o compartilhamento de bases de dados públicos para finalidades além daquelas inicialmente previstas na coleta atrai os limites da decisão do Supremo Tribunal Federal em 2022 acima descrito. Ainda que todas as informações sejam públicas, o uso delas pelos órgãos de fiscalização aduaneira podem estão aos parâmetros e efeitos estabelecidos nessa decisão.

Ainda sobre sistema de inteligência artificial que utilizam dados pessoais, o sistema IRIS realiza reconhecimento facial de viajantes¹⁷. A própria Receita Federal disponibilizou em seu canal oficial da plataforma de YouTube vídeo sobre o sistema¹⁸, informando que o sistema recairá “preferencialmente sobre passageiro que apresentem riscos em potencial de estarem praticando irregularidades aduaneiras, reconhecendo automaticamente e permitindo uma fiscalização mais aprofundada”. Em notícia sobre o sistema, o SERPRO menciona “De posse dos dados biográficos de passageiros/tripulantes, o e-DBV está apto a realizar o reconhecimento facial, identificar o perfil do viajante e fornecer informações aos agentes da alfândega.” (Brasil, [202-]).

Percebe-se que, portanto, que a constitucionalização da proteção de dados no Brasil inaugura uma nova ordem jurídica que impõe novas análises pelos agentes responsáveis pela fiscalização tributária.

Essas análises já podem ser realizadas seguindo as diretrizes do Supremo Tribunal Federal para tratamentos de dados pessoais pelo Estado, e com o auxílio do conteúdo do julgamento da Corte de Justiça da União Europeia no Caso C-175/20 para o contexto da fiscalização tributária.

Seguindo esses parâmetros de maneira preventiva como forma de demonstrar a adequação à Lei Geral de Proteção de Dados Pessoais, além dos órgãos competentes evitarem a anulação de algumas de suas atividades, os servidores públicos também podem evitar possíveis indenizações ao Estado, conforme mencionado em julgamento do Supremo Tribunal Federal citado anteriormente.

¹⁷ Documento sobre o funcionamento do sistema foi elaborado por ofício da Auditora Fiscal Cláudia Maria de Andrade. Disponível em <https://repositorio.enap.gov.br/bitstream/1/4132/1/Projeto%20IRIS%20-%20Reconhecimento%20Facial%20de%20Viajantes.pdf>. Acesso em 04 de outubro de 2022.

¹⁸ BRASIL. Receita Federal. O Sistema de Reconhecimento Facial do Projeto Iris. 14 de dezembro de 2016. Disponível em <https://www.youtube.com/watch?v=6eJVpxe0pxY>. Acesso em 29 de novembro de 2022.

Considerações finais

A construção do direito fundamental à autodeterminação informacional pelo Tribunal Constitucional da Alemanha em 1983 foi resultado de preocupações com uma nova realidade de sistemas informacionais que os Estados estavam descobrindo, possibilitando novos mecanismos de monitoramento social.

A sanção à autoridade de fiscalização tributária da Holanda demonstra que um direito fundamental à proteção de dados pessoais deve impor limites claros e objetivos quanto à tratamentos realizados por entes de fiscalização tributária, ainda que no seu desempenho da função de garantir a observância do princípio da capacidade contributiva dos cidadãos.

Nesse contexto, o advento da EC 115/22, consagrando o direito fundamental à proteção de dados, não é inócuo ou indiferente ao sistema e à fiscalização tributária, mas incide diretamente nestas atribuições estatais. O presente artigo demonstrou que são indispensáveis ajustes e adaptações na administração tributária, principalmente quanto à fiscalização, observando a proteção de dados pessoais não só nos seus requisitos infraconstitucionais previstos na Lei Geral de Proteção de Dados, como também no seu elemento de direito fundamental por meio da aplicação dos princípios que compõem esse direito.

Referências

BRASIL. Receita Federal. **O Sistema de Reconhecimento Facial do Projeto Iris**. 14 de dezembro de 2016. Disponível em: <https://www.youtube.com/watch?v=6eJVpxe0pxY>. Acesso em: 29 nov. 2022.

BRASIL. SERPRO. **Reconhecimento facial intensifica segurança nos aeroportos**. [202-]. Disponível em: <http://intra.serpro.gov.br/tema/noticias-tema/reconhecimento-facial-intensifica-seguranca-nos-aeroportos> . Acesso em: 29 nov. 2022.

BRASIL. Supremo Tribunal Federal. **Ação Direta de Inconstitucionalidade 6649 e Arguição de Descumprimento de Preceito Fundamental 695**. Brasília. 15 de setembro de 2022. Disponível em: <https://images.jota.info/wp-content/uploads/2022/09/voto-adi-6649-e-adpf-695-1.pdf> . Acesso em: 05 out. 2022.

BRASIL. Supremo Tribunal Federal. **Recurso Extraordinário nº 601.314**. 24 de fevereiro de 2016. Brasília. Disponível em: <https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=11668355> . Acesso em: 26 abr. 2022.

BRASIL. Supremo Tribunal Federal. **Referendo em Medida Cautelar nas ADIS 6.387, 6.388, 6.389, 6.390 e 6.393**. Brasília. 07 de maio de 2020. Disponível em: <https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=754358567>. Acesso em: 26 abr. 2022.

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico Journal of Law [EJLL]**, v. 12, n. 2, p. 91-108, 2011. Disponível em: <https://periodicos.unoesc.edu.br/espacojuridico/article/view/1315/658> . Acesso em: 30 jan. 2023.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**: fundamentos da lei geral de proteção de dados. rev. e atual. São Paulo: Thomson Reuters Revista dos Tribunais, 2019.

FUCK, Luciano Felício. **Estado Fiscal e Supremo Tribunal Federal**. São Paulo: Saraiva, 2017.

HESSE, Konrad. **Grundzüge des Verfassungsrechts der Bundesrepublik Deutschland**. Heidelberg: C. F. Müller, 1999.

HOFFMANN-RIEM, Wolfgang. **Teoria geral do direito digital**: transformação digital desafios para o direito. Forense, 2021.

JAMBEIRO FILHO, Jorge Eduardo de Schoucair. Inteligência Artificial no Sistema de Seleção Aduaneira por Aprendizado de Máquina. **Secretaria da Receita Federal do Brasil**, v. 14, 2019. Disponível em: <https://repositorio.enap.gov.br/bitstream/1/4622/1/1º%20lugar%20do%2014º%20Premio%20RFB.pdf>. Acesso em: 04 out. 2022.

JANINI, Tiago Cappi; PULCINELLI, Ana Luiza Godoy. A fiscalização tributária e seus limites: uma análise a partir do princípio da legalidade e dos direitos fundamentais do contribuinte. **Revista de Direito Tributário e Financeiro**, n. 2, p. 349, 2016.

JARUDE, Jamile Nazaré Duarte Moreno. **O estado da arte da fiscalização tributária federal e o uso de inteligência artificial**. Dissertação (Mestrado em Direito), Universidade de Marília, São Paulo, 2020. Disponível em: <https://repositorio.enap.gov.br/handle/1/6415>.

LUXEMBURGO. **Corte de Justiça da União Europeia**. Caso C-175/20. 24 de fevereiro de 2022. Disponível em: <https://curia.europa.eu/juris/document/document.jsf?text=&docid=254583&pageIndex=0&doclang=PT&mode=lst&dir=&occ=first&part=1&cid=340057>. Acesso em: 15 fev. 2023.

MALDONADO, Luciano Burti. Limites do Poder de Fiscalização: Identificação e Controle. **Revista Direito Tributário Atual**, n. 45, p. 264-288, 2020.

MALDONADO, Luciano Burti. LIMITES DO PODER DE FISCALIZAÇÃO: MARTINS, Ives Gandra da Silva. Sigilo bancário e privacidade. *In*: SARAIVA FILHO, Oswaldo Othon de Pontes; GUIMARÃES, Vasco Branco (coord.). **Sigilos bancário e fiscal**: homenagem ao Jurista José Carlos Moreira Alves. Belo Horizonte: Fórum, 2011.

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

MENDES, Laura Schertel Ferreira. Autodeterminação informativa: a história de um conceito. **Pensar-Revista de Ciências Jurídicas**, v. 25, n. 4, 2020.

POSSA, Alisson; RAMOS, Julia L. Risco de crédito e o direito a revisão de decisões automatizadas: uma sistematização de elementos mínimos a serem observados em tratamentos de scoring de crédito. *In*: **Revista Jurídica do Banco do Nordeste**. Ceará: Banco do Nordeste, Ano 11, nº 6, p. 43-40, 2022.

SCARCELLA, Luisa. Tax compliance and privacy rights in profiling and automated decision making. **Internet Policy Review**, 8, (4), 2019.

VÉLIZ, Carissa. Why Democracy Needs Privacy. **Boston Review**. 2021. Disponível em <https://bostonreview.net/articles/why-democracy-needs-privacy/>. Acesso em: 26 abr. 2022.

WARREN, Samuel *et al.* Louis Brandeis. The Right to Privacy. **Harvard Law Review**, v. 4, n. 5, p. 193-220, 1890.