JOSÉ VALMI BRITO

O uso de dados pessoais pelo setor público e as administrações tributárias no contexto da LGPD

Dissertação apresentada como requisito parcial para obtenção do título de Mestre em Direito

Área de concentração: Direito, Justiça e Desenvolvimento

Orientador: Professor Flávio Henrique Unes Pereira

Instituto Brasiliense de Direito Público

São Paulo

2021

Nome: BRITO, José Valmi

Título: O uso de dados pessoais pelo setor público e as administrações tributárias no contexto da LGPD

Dissertação apresentada ao Instituto Brasiliense de Direito Público para obtenção do título de Mestre em Direito.

Aprovado em: _____

Banca Examinadora

Prof. Dr. _____ Instituição: _____

Julgamento: _____ Assinatura: _____

Prof. Dr. _____ Instituição: _____

Julgamento: _____ Assinatura: _____

Prof. Dr. _____ Instituição: _____

Julgamento: _____ Assinatura: _____

Dedico, com saudade, este trabalho aos meus pais. Embora ausentes fisicamente, sempre estiveram espiritualmente presentes, transmitindo-me muita força e determinação. Sei que onde quer que estejam estão orgulhosos.

AGRADECIMENTOS

Gostaria de agradecer a todos aqueles que contribuíram para a execução desta longa etapa, o Mestrado em Direito, que neste momento se aproxima do fim com a entrega desta dissertação.

Este trabalho não seria possível sem a ajuda e colaboração de um conjunto de pessoas, que possibilitaram tornar esse sonho realidade. Por essa razão, a todas presto meu agradecimento.

Primeiramente, em especial, aos meus pais, que sempre contribuíram para o meu sucesso. Sem o apoio deles, provavelmente eu não estaria aqui, uma vez que sempre incentivaram meus estudos e disponibilizaram tudo o que era necessário para meu sucesso escolar. Também aos meus amigos, que ajudaram e demonstraram carinho e amizade ao longo de todo o percurso acadêmico.

À minha esposa, que, com seu gênio forte, correto, sincero, verdadeiro, muitas vezes assumindo o papel de minha mãe, fez com que eu almejasse cada vez mais estar vivendo este momento.

Às minhas filhas, que, cada uma à sua maneira, e com todo o carinho que lhes é característico, aconchegaram-me durante este processo.

Ao meu filho, que, com seu simples nascimento, trouxe-me maturidade suficiente para atravessar fronteiras jamais transpostas.

Não posso deixar de agradecer ao meu orientador, Prof. Flávio Henrique Unes Pereira. Sou grato pela disponibilidade e dedicação na orientação deste trabalho, bem como toda a motivação que sempre me deu e confiança que depositou em mim.

Os meus agradecimentos são também destinados ao Instituto Brasiliense de Direito Público, por todo o percurso acadêmico proporcionado, e aos professores que aceitaram colaborar com este trabalho de investigação.

Aos demais, que direta ou indiretamente, de alguma forma, deram o seu contributo para que eu chegasse com sucesso ao fim desta etapa: a todos, o meu sincero agradecimento.

RESUMO

O objetivo deste trabalho é analisar o fenômeno normativo recente da proteção de dados pessoais e privacidade no setor público, verificando como isso afetará, em especial, o uso de dados pessoais no direito tributário, com um breve estudo sobre as administrações tributárias. Para tanto, começa-se a tratar da tutela constitucional do direito à privacidade e as normas infraconstitucionais a respeito, culminando na análise da novel Lei Geral de Proteção de Dados Pessoais – LGPD. Em um segundo momento, é feita a intersecção entre o direito tributário e a proteção de dados pessoais, trazendo as principais questões do primeiro ramo que podem ser afetadas pelo segundo. O trabalho explora ainda os deveres das administrações tributárias em relação à proteção de dados pessoais e verifica como a atividade de exação tributária pode ser afetada pela LGPD. Por fim, explora-se questões relativas a normas e disciplinas específicas de proteção de dados que impactam o direito público brasileiro, com uma análise sobre a necessidade de uma "LGPD Tributária".

Palavras-chave: Proteção de dados pessoais; direito público; administração tributária; proteção ao contribuinte.

ABSTRACT

This paper aims to analyze the recent phenomenon of personal data protection and privacy legislation with public law, verifying how it will affect personal data in the context of Taw Law (with a brief study related to the tax administrations). To this end, it begins to deal with the constitutional protection of the right to privacy and its regulation, culminating in analyzing the new General Law for the Protection of Personal Data - LGPD. The second step is an intersection between tax law and personal data protection, bringing up the first main issues that may be affected by the second. Still, the paper explores tax administration duties concerning protecting personal data and seeing how the LGPD may influence taxation activity. Finally, this dissertation deals with specific data protection rules that impact the Brazilian public law, with an analysis on the need for a “Tax LGPD.”

Keywords: Data privacy; public law; tax authority; rights to the taxpayers.

LISTA DE ABREVIATURAS E SIGLAS

ABREVIATURA OU SIGLA	SIGNIFICADO
ADI	Ação Direta de Inconstitucionalidade
ANATEL	Agência Nacional de Telecomunicações
ANPD	Autoridade Nacional de Proteção de Dados Pessoais
AO	*Abgabenordnung* (Código Tributário Alemão)
BfDI	*Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit* (Autoridade Federal Alemã de Proteção de Dados)
BVerfG	*Bundesverfassungsgericht* (Tribunal Constitucional Alemão)
CARF	Conselho Administrativo de Recursos Fiscais
CCPA	*California Consumer Privacy Act*
CERT.br	Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil
COAF	Conselho de Controle de Atividades Financeiras
CTN	Código Tributário Nacional
CVM	Comissão de Valores Mobiliários
DEM	Democratas
e-MSF	Manual Eletrônico do Sigilo Fiscal
ENISA	*European Union Agency for Cybersecurity*
GDPR	*General Data Protection Regulation*

GT29	Grupo de Trabalho 29
IBGE	Instituto Brasileiro de Geografia e Estatística
ISO	*International Organization for Standardization*
LAI	Lei de Acesso à Informação
LGPD	Lei Geral de Proteção de Dados Pessoais
MCI	Marco Civil da Internet
NIST	*National Institute of Standards and Technology*
OAB	Ordem dos Advogados do Brasil
OWASP	*Open Web Application Security Project*
PAD	Processo Administrativo Disciplinar
PEC	Proposta de Emenda à Constituição
PL	Projeto de Lei da Câmara dos Deputados
PLS	Projeto de Lei do Senado Federal
PSB	Partido Socialista Brasileiro
PSDB	Partido da Social Democracia Brasileira
PSOL	Partido Socialismo e Liberdade
RGPD	Regulamento Geral de Proteção de Dados Pessoais
RJET	Regime Jurídico Emergencial e Transitório das Relações Jurídicas de Direito Privado

SUMÁRIO

Introdução

Em 6 de maio de 2017, a renomada revista *The Economist* (2017) publicou uma reportagem relatando que o recurso mais valioso do mundo não era mais o petróleo, e sim dados. Colocando na capa as principais companhias de tecnologia do planeta (Amazon, Apple, Microsoft, Google, Facebook, Tesla), ficou evidente para o leitor do periódico que o paradigma do mundo havia mudado: as maiores empresas, a partir de então, são as que tratam dados pessoais, e não mais as tradicionais do setor de petróleo, como as históricas Sete Irmãs (hoje consolidadas em Shell, BP, ExxonMobil e Chevron).

Porém, enquanto o setor de óleo e gás é altamente regulado pelo Estado – fruto de uma evolução nos Estados Unidos desde o século XIX com o trabalho dos principais empresários do setor (como John Davidson Rockefeller com a *Standard Oil*, por exemplo) –, as principais empresas de tecnologia surgiram há cerca de vinte anos. Exceto Apple e Microsoft, criadas nos anos 1970, as demais começaram a surgir e se desenvolver apenas na década de 1990.

Tais pessoas jurídicas se beneficiaram enormemente da evolução da internet em escala global, também ocorrida a partir da mesma década de 1990, sobretudo com a popularização do computador doméstico. Com o uso da rede mundial de computadores se tornando mais frequente, fazer negócios no meio virtual foi ficando cada vez mais fácil para as organizações. A internet passou a servir não apenas para checar e-mails ou entrar em salas de bate-papo, mas como uma ferramenta para promover atividades econômicas altamente lucrativas.

No início deste século, o Facebook – que atualmente mudou o nome para Meta – revolucionou o conceito de uso da internet com as redes sociais. Embora já existentes em outras plataformas, como o Orkut, a interface amigável do produto capitaneado por Mark Zuckerberg ajudou a trazer cada vez mais usuários para esse tipo de atividade virtual.

Mas foi, deveras, nesta última década de 2010 que as relações virtuais atingiram outro patamar. Com a popularização de aplicativos de mensagens – como WhatsApp, Messenger e Telegram –, o surgimento de outras redes sociais com finalidades distintas – como o Instagram e o LinkedIn –, além de plataformas em

que qualquer indivíduo pode expressar amplamente suas ideias – como o Twitter – , o "oceano" de dados pelo qual as empresas podem "navegar" aumentou consideravelmente, trazendo preocupações em relação ao risco de manipulação de pessoas por meio do capitalismo de vigilância[1]. De igual maneira, isso vem trazendo debates importantes sobre a influência das redes sociais na vida das pessoas[2].

As autoridades, igualmente preocupadas com o que a desregulamentação na internet poderia gerar nesse mundo massivo de dados, começaram a se movimentar para acompanhar a tendência. A União Europeia tomou a iniciativa, com a publicação do seu Regulamento Geral de Proteção de Dados Pessoais, conhecido pelo acrônimo em inglês GDPR (ou RGPD em português). Sua promulgação ocorreu em 2016, no contexto do escândalo da *Cambridge Analytica*, que colocou em suspeição processos eleitorais no mundo inteiro, em especial o presidencial dos Estados Unidos da América e o plebiscito do Brexit, no Reino Unido. O tema ganhou destaque global[3] e o Senado norte-americano promoveu uma audiência com Mark Zuckerberg, visto que o Facebook esteve envolvido neste escândalo, a fim de prestar maiores esclarecimentos sobre o tema. Ou seja, o assunto passou a ser lugar comum nas discussões sobre privacidade e proteção de dados na sociedade.

Em 2018, o Estado da Califórnia decidiu também promulgar o *California Consumer Privacy Act* – CCPA, para reforçar as questões de privacidade dos titulares de dados pessoais.

O Brasil, na esteira do que estava acontecendo nos Estados Unidos e na União Europeia, promulga, em 14 de agosto de 2018, a Lei Geral de Proteção de Dados Pessoais – LGPD. Com isso, o paradigma brasileiro em relação à privacidade e à proteção de dados pessoais também passa a mudar – embora em marcha lenta – e deve ser a tônica das relações jurídicas da terceira década do século XXI.

---

[1] Expressão cunhada pela autora Shoshana Zuboff, que relaciona o capitalismo moderno com o uso intensivo de dados.
[2] O assunto foi trazido em NETFLIX, 2020.
[3] Além disso, virou documentário que trouxe a disseminação da discussão (NETFLIX, 2019).

É nessa linha que esse trabalho tenta propor uma abordagem da interferência da LGPD nas relações tributárias. Embora o ritmo de mudança de paradigma seja maior no setor privado, é certo que a LGPD revolucionará a maneira como o setor público trata dados pessoais.

Contudo, é certo que o setor público brasileiro – sobretudo no caso das administrações tributárias – não coloca o tema da privacidade e proteção de dados pessoais como prioridade máxima em seus misteres públicos. Uma porque o *enforcement*, ou seja, a força e aplicação da lei é reduzida no nosso direito em comparação com essas experiências internacionais; duas porque o sistema federativo brasileiro, com três níveis autônomos, prejudica um esforço nacional em um assunto que não afeta apenas o Governo Federal.

Como consequência, não raro é possível observar, por parte de órgãos públicos, violações em relação à privacidade e proteção de dados, falhas constantes em segurança da informação, vazamentos de dados pessoais, dentre outros problemas que acometem a Administração Pública brasileira. E isso também constitui incentivo para que *hackers* se aproveitem da situação, o que foi amplamente observado no contexto da pandemia de Covid-19 e a proliferação de incidentes que ocorreram em 2020 e 2021 nos mais diversos órgãos públicos[4].

O maior problema da atividade tributária brasileira é o diálogo mais árduo que é feito com outras searas do Direito, o que faz com que a disciplina ganhe um caráter quase que autônomo no direito pátrio. Dessa maneira, embora se conceba a ciência do Direito de maneira sistêmica, no caso do direito tributário ele ganha maior força por representar o interesse público na correta aplicação da tributação na sociedade.

A consequência disso é que o direito tributário exibe princípios e métodos interpretativos próprios. Com isso, sofre influxo muito sutil e discreto de normas de outros campos, tal como o direito privado, e isso é perceptível em julgamentos administrativos, em que o foco acaba sendo muito constante na faceta tributária e menos no direito adjacente que consubstancia a relação jurídica tributária.

[4] O caso mais ilustrativo ocorreu no site do Ministério da Saúde, onde um ransomware impediu milhões de brasileiros de terem acesso às informações sobre a vacinação durante o período em que ficou indisponível para acesso (CNNBRASIL, 2021).

Nesse sentido, a principal contribuição deste trabalho é correlacionar as fontes do direito tributário com a seara da privacidade e proteção de dados, dando destaque para esta última, em como ela pode afetar o dia a dia das diversas administrações tributárias no país. Como um microssistema jurídico, a privacidade e proteção de dados pessoais traz diversos impactos no macrossistema do direito tributário.

O tema é bastante interdisciplinar e exige, portanto, a interação com diversas áreas do saber. Conforme apontam ROCHA e UNES PEREIRA (2021b, p. 116):

> A interdisciplinaridade engrandece e contribui para o desenvolvimento de qualquer ramo do conhecimento, e o Direito não se constitui em exceção, certo que historicamente tem ele se valido de valiosas contribuições de outros campos como os da filosofia, sociologia, psicologia, antropologia, apenas para citar os mais influentes. [...]

Neste trabalho, portanto, haverá a busca por fontes da ciência do Direito, mas também serão utilizados conhecimentos de Administração, Segurança da Informação e Tecnologia da Informação, haja vista que privacidade e proteção de dados pessoais interferem nessas diversas temáticas.

A metodologia adotada nesta dissertação profissional é a pesquisa exploratória, com a revisão de bibliografia mais abrangente sobre LGPD e da pouca jurisprudência já existente sobre o tema no País. Também será feito um estudo comparativo com o impacto do GDPR no direito tributário alemão, em especial com base no trabalho seminal de SEER (2020), bem como o artigo de SERAFINO (2020) enfocado no aspecto do tratamento de dados pessoais para fins tributários.

A escolha pela Alemanha como ponto de análise se deu em razão da existência de uma norma europeia similar à LGPD incidindo nas relações jurídicas tributárias, que é o GDPR, e devido ao debate doutrinário do direito tributário alemão em relação à proteção de dados pessoais estar em um grau de maturidade elevado, o que pode servir de paradigma para o debate brasileiro sobre a LGPD. O texto de Seer expõe, por exemplo, diversos questionamentos que são amplamente válidos para o direito público brasileiro na esfera tributária.

Além dessa literatura específica, a pesquisa fará críticas pontuais em relação à LGPD e às suas dificuldades na interação com o ramo do direito público brasileiro, justamente por ter sido uma norma mais voltada para empresas e menos ao Estado. Outro ponto de atenção é que a própria redação da LGPD gera muitas dúvidas interpretativas. São esses os problemas nucleares que esta dissertação procura demonstrar.

Uma possível solução discutida no final do trabalho é a elaboração de normas específicas para o setor público. Será, portanto, explorada se há necessidade de uma "LGPD Tributária" no país à luz das discussões ocorridas no direito alemão.

A abordagem proposta adota uma perspectiva da práxis do direito público (incluindo o tributário) brasileiro e não necessariamente está pautada em um debate jusfilosófico, visto que não há, até o momento, produção acadêmica suficiente no país para um debate científico do tema – diferentemente do contexto alemão, como se observou. Logo, tal enfoque pragmático vai ao encontro dos objetivos de um mestrado profissional em Direito.

O trabalho está dividido em dois capítulos. O primeiro tem como objetivo expor a proteção de dados pessoais no Brasil e toda a sua tutela jurídica, que ocorreu nos últimos dez anos com o surgimento de leis que abordavam o assunto, até culminar na LGPD.

O segundo capítulo traz a relação da tributação com a proteção de dados pessoais, explorando questões como o segredo comercial e industrial e o sigilo fiscal e bancário, além do compartilhamento de dados pessoais entre órgãos públicos – os quais podem ser usados para fins tributários. Também se discute a função da LGPD como norma geral e o surgimento de leis específicas sobre tratamento de dados, como o caso da MP 954/2020, e ainda se é necessária uma "LGPD Tributária" ou uma compatibilização com o atual Código Tributário Nacional.

Em termos formais, esclarecemos que todos os grifos contidos nas citações são reproduções do original (a não ser que haja menção em sentido contrário); todas as siglas utilizadas foram previamente definidas quando de seu primeiro uso no corpo do texto e também constam na lista de siglas e abreviaturas; e optamos pelo método de citação autor-data, com o uso exclusivo do sobrenome do autor, para dar maior fluidez à leitura. Os destaques em negrito em textos não

reproduzidos são do próprio autor, e as palavras em itálico representam expressões em latim ou em idioma estrangeiro.

1. A proteção de dados pessoais e sua tutela jurídica no Brasil

Privacy is the right to a free mind.

Edward Snowden, em debate com Noam Chomsky e Glenn Greenwald (In: 35:21). Disponível em: <https://vimeo.com/160952562>. Acesso em: 28 jun. 2021.

1.1. O direito à privacidade em uma perspectiva comparada

O direito à privacidade, historicamente delineado por WARREN e BRANDEIS (1890), é expresso pelo direito de não ser incomodado. Trata-se de um dos pilares de qualquer sociedade democrática, visto que a falta de privacidade implicaria um controle estatal da informação e da vida das pessoas em sociedade. Na verdade, foi com esse trabalho inaugural que a discussão da privacidade começou a ser abordada sob o aspecto jurídico nos Estados Unidos, visto que o tema não era amplamente tratado na comunidade jurídica.

LÓSSIO (2021, p. 63) expõe que o texto dos autores mencionados anteviu diversas tendências em relação ao direito à privacidade no século XX. Inclusive, destaca o autor, o trabalho teve influência no artigo 12 da Declaração Universal dos Direitos Humanos[5] e se antecipou à popularização do telefone nos Estados Unidos, bem como às práticas de escutas telefônicas. Posteriormente, em um caso da Suprema Corte norte-americana (Olmstead v. Estados Unidos) Brandeis acabou defendendo fortemente o direito à privacidade em uma situação de conversa telefônica.

No âmbito europeu, o início da discussão relativa à privacidade costuma ser relacionada com a Revolução Francesa e a busca, pelos cidadãos, de menor interferência do Estado em suas vidas (BRASIL, 2018). Nesse sentido, a ideia da privacidade é mais ligada aos ideais liberais daquele período. Na Alemanha, por sua vez, o célebre caso sobre a Lei do Censo de 1983 fez com que o Tribunal Constitucional Federal Alemão reconhecesse o direito à autodeterminação informativa[6] como corolário do próprio direito à privacidade, conforme relata SEER (2020, p. 23). Portanto, juntamente com o texto seminal de WARREN e BRANDEIS, esse é o grande marco jurídico europeu sobre a temática.

Na realidade, até pouco tempo, a privacidade não era concebida como um conceito relevante a ser tratado juridicamente, o que demonstra ser uma

[5] “Ninguém será sujeito à interferência na sua vida privada, na sua família, no seu lar ou na sua correspondência, nem a ataque à sua honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques.”
[6] O conceito será mais bem delineado adiante.

preocupação recente das sociedades modernas, em especial com o delineamento do conceito de intimidade.

Convém destacar as nuances trazidas no que se refere à privacidade e intimidade, algo mais restrito. Conforme descreve PAULSEN (2020, p. 358) sob o aspecto constitucional:

> Conforme GONET BRANCO, "há consenso em que o direito à privacidade tem por característica básica a pretensão de estar separado dos grupos, mantendo-se o indivíduo livre da observação de outras pessoas". Esse autor ressalta, forte em doutrina norte-americana, que WILLIAM PROSSER teria sustentado quatro meios básicos de afrontar a privacidade: "a) intromissão na reclusão ou na solidão do indivíduo, 2) exposição pública de fatos privados, 3) exposição do indivíduo a uma falsa percepção do público (*false light*), que ocorre quando a pessoa é retratada de modo inexato ou censurável, 4) apropriação do nome e da imagem da pessoa, sobretudo para fins comerciais". Estreitando o sentido, aponta que o direito à privacidade "conduz à pretensão do indivíduo de não ser o foco da observação por terceiros, de não ter os seus assuntos, informações pessoais e características particulares expostas a terceiros ou ao público em geral".
>
> A intimidade, por si, constitui um espaço ainda mais exclusivo, relacionado ao ser humano no âmbito da sua individualidade, seja física, emocional ou intelectual, alcançando o que diz respeito ao seu corpo, à sua sexualidade, aos seus relacionamentos e aos seus pensamentos.

O direito à privacidade, apesar de historicamente se tratar de uma liberdade negativa dentro da conceituação de Isaiah Berlin,[7] no mundo moderno precisa ser complementado por outros direitos para que pudesse ter plena efetividade. Não é um direito que se efetiva por si só, como no passado, bastando que o Estado não incomodasse o particular e protegesse sua privacidade de violações de terceiros.

Com o desenvolvimento das telecomunicações, o surgimento do uso da internet e sua popularização a partir dos anos 1990, o direito à privacidade passou a ter que ser tutelado no meio virtual, visto que este "novo mundo" virou uma extensão da vida "no mundo real" do indivíduo. Foi o início, portanto, de uma

[7] Segundo RAMOS (2011, p. 257), a liberdade negativa é a ideia de que a pessoa está livre para fazer o que for possível onde não houver restrições ou impedimentos. Como exemplos, podem ser citadas as liberdades de expressão e de associação.

mutação do conceito de privacidade desenvolvido na Revolução Francesa e depois tratado nos EUA no século XIX.

Um comentário ofensivo uma rede social tem repercussões na esfera íntima e psicológica do outro. Não se trata de um território sem lei ou de um mundo fictício, como é o caso de jogos de videogame, em que basta desligar o aparelho para que tudo aquilo termine e a vida siga no mundo real. Há repercussões permanentes nas condutas virtuais.

O direito, no entanto, não acompanhou *pari passu* essas evoluções tecnológicas, ficando o mundo virtual teoricamente mais suscetível a violações de privacidade dos indivíduos. Faltou também uma uniformização da legislação que trata do tema, conforme dispõe LEONARDI (2019, p. 30), o que tem prejudicado o tratamento jurídico mais efetivo sobre o assunto:

> Do ponto de vista pragmático, a solução pareceria perfeita. Se todas as nações do mundo concordassem em adotar uma legislação global única para a Internet, a vida dos usuários, dos provedores de serviços e das empresas se tornaria muito mais simples. Não haveria conflitos entre leis no espaço nem necessidade de conhecer e cumprir normas oriundas de todas as nações do mundo. Além disso, seria possível evitar a criação de "paraísos digitais", ou seja, territórios de regulação inexistente ou tolerante com relação à prática de atos ilícitos por meio da internet.

É perceptível que, quando um *paparazzo* invade o jardim de uma casa para fotografar a intimidade de uma celebridade, ele está violando sua privacidade;[8] o mesmo raciocínio, contudo, não costuma ser feito no mundo virtual. Metaforicamente, muitas empresas se aproveitaram para invadir de maneira constante o "jardim virtual" alheio, violando a privacidade dos titulares sem qualquer remorso, em especial por meio do uso de seus dados pessoais – que possuem imenso potencial econômico. As companhias no ambiente virtual não estão interessadas em explorar a intimidade de maneira sensacionalista como um

[8] Tal invasão de privacidade é bem representada pela cobertura feita pelos tabloides britânicos da família real. O caso de maior repercussão foi o acidente automobilístico sofrido por Diana, Princesa de Gales, em 1997, em Paris, em virtude da perseguição de *paparazzi* a seu veículo.

paparazzo, porém, são mais sutis ao querer explorar dados pessoais que lhes possibilitam aumentar sua lucratividade.

Nesse sentido, não há como negar que a proteção de dados pessoais seja um direito intimamente associado ao direito à privacidade, também caminhando de maneira harmoniosa:

> Até mesmo o produto mais importante da primeira geração de leis sobre o tratamento automático das informações, o direito de acesso, deu origem a consequências e perspectivas não previstas originalmente, que vão além da restrita tutela da esfera privada individual. Ao se oferecer aos indivíduos um meio dinâmico para salvaguardar o próprio patrimônio informativo, abriu-se igualmente o caminho que fez caírem as barreiras de sigilo que circundavam as informações mantidas por outros sujeitos. As leis sobre proteção de dados cumpriram um papel prenunciador para as leis sobre a liberdade de acesso às informações em mãos públicas, sobre a administração 'à luz do sol': e disto derivou uma importante modificação do quadro geral, no sentido de que a ênfase foi sendo colocada, progressivamente, mais do que na defesa da esfera individual, em regras gerais de circulação das informações, pessoais ou não, sob o controle público. (RODOTÀ, 2008, p. 44)

A preocupação de conjugar a tutela da privacidade com a dos dados pessoais começou a ficar mais clara juridicamente nos últimos anos. O direito, acompanhando a tecnologia, começa a se pronunciar sobre tais condutas. Cumpre destacar que houve maior profusão de normas a partir da década de 1990 – justamente em razão da maior digitalização da economia mundial:

> O motivo que inspirou o surgimento de regulamentações de proteção de dados pessoais de forma mais consistente e consolidada a partir dos anos 1990 está diretamente relacionado ao próprio desenvolvimento do modelo de negócios da economia digital, que passou a ter uma dependência muito maior dos fluxos internacionais de bases de dados, especialmente os relacionados às pessoas, viabilizados pelos avanços tecnológicos e pela globalização.
>
> Desse modo, houve a necessidade de resgatar e repactuar o compromisso das instituições com os indivíduos, cidadãos desta atual sociedade digital, no tocante à proteção e à garantia dos direitos humanos fundamentais, como o da privacidade, já celebrados desde a

> Declaração Universal dos Direitos Humanos (DUDH) de 1948. (PINHEIRO, 2020, p. 17)

No âmbito da União Europeia, onde há, assim como os EUA, uma tradição histórica na proteção de dados pessoais, a Carta dos Direitos Fundamentais da União Europeia (2000/C 364/01) destaca a complementaridade entre os direitos à privacidade e proteção de dados pessoais em seus artigos 7º e 8º, conforme a seguir:

> Artigo 7.º
>
> Respeito pela vida privada e familiar
>
> Todas as pessoas têm direito ao respeito pela sua vida privada e familiar, pelo seu domicílio e pelas suas comunicações.
>
> Artigo 8.º
>
> Proteção de dados pessoais
>
> 1. Todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito. 2. Esses dados devem ser objeto 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. 3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente.

Como se depreende, a União Europeia imprime uma estatura supralegal ao direito à proteção de dados, trazendo reforço ao direito à privacidade contido no artigo 7º. Com isso, ganha-se relevância a tutela jurídica da União Europeia.

Após constar expressamente na Carta dos Direitos Fundamentais, a União Europeia promulgou o Regulamento Geral de Proteção de Dados Pessoais (2016/679) do Parlamento Europeu e do Conselho, em 27 de abril de 2016, conhecido como GDPR. Com isso, a antiga Diretiva 95/46/CE foi revogada pelo novo diploma, passando a ser autoaplicável em todos os Estados-Membros da UE.

O Regulamento, à diferença das diretivas, não exige a internalização pelos Estados-Membros, tendo aplicação imediata (SEER, 2020, p. 27).

1.2. A normativa brasileira sobre privacidade antes da LGPD

O Brasil é um país que concede estatura constitucional ao direito à privacidade, como diversas outras nações do mundo. Nisso é possível afirmar que nossa Constituição não exibe omissões no que se refere ao tema. O artigo 5º, inciso X, da Constituição da República Federativa do Brasil prescreve que "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas".

É importante destacar que a proteção de dados pessoais nunca possuiu estatura constitucional, tal como se verifica na União Europeia, embora existam iniciativas legislativas infraconstitucionais mais recentes a respeito. A opção tem sido, portanto, por esta via legislativa.

Em contrapartida, cumpre destacar a Proposta de Emenda à Constituição (PEC) nº 17/2019 aprovada em 2021, que inclui o referido direito na Carta Constitucional brasileira por meio de alteração do artigo 5º, XII. O dispositivo contará com a seguinte redação:

> Art. 5º .....
> .....
>
> XII – é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal, **bem como é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais**;
> .....
> (NR) (grifo nosso)

Portanto, como veremos adiante, o Brasil consolidou o marco legal em proteção de dados pessoais em 2018 sem possuir internalizado o marco

constitucional no que se refere ao tópico – o que se faz posteriormente com a supramencionada PEC. Isso culminou na regulamentação trazida pela Lei nº 13.709/2018.

É relevante compreender a tutela infraconstitucional da proteção de dados pessoais, já que, como exposto, o regime constitucional do tema é focado somente no direito à privacidade, intimidade, honra e imagem, e quaisquer menções ao tema de proteção de dados nessa esfera constitucional têm sido *de lege ferenda*.

Por essa razão, convém fazer uma análise dogmática de pelo menos três leis que influenciaram diretamente o tema: a Lei de Acesso à Informação – LAI, o Marco Civil da Internet – MCI, e a Lei Geral de Proteção de Dados Pessoais – LGPD. Esses marcos normativos servem de baliza para que se possa compreender a estrutura de proteção à privacidade e proteção de dados pessoais no Brasil.

Os dois primeiros marcos normativos (LAI e MCI) podem ser considerados como emitidos em um contexto "pré-GDPR" no Brasil, ou seja, em uma situação ainda incipiente em relação à regulamentação do tratamento dos dados pessoais. Afinal, a norma europeia, que serviu de inspiração direta para a LGPD, ainda não havia sido promulgada. A partir de 2016, com a sua promulgação, temos um contexto pós-GDPR, em que a tutela do tratamento dos dados pessoais passa a ser mais específica (no caso da LAI e do MCI ela é residual). É nesse contexto que surge a LGPD, como veremos adiante.

1.2.1. A Lei de Acesso à Informação – LAI (Lei nº 12.527/2011)

Como destacado no item anterior, coube à legislação infraconstitucional brasileira estruturar o marco legal de proteção de dados pessoais no país. Porém não foi com a LGPD que a disciplina jurídica ganhou força neste século; é um movimento que vem ocorrendo há mais de uma década.

Uma das primeiras iniciativas nessa direção é a Lei de Acesso à Informação – LAI (Lei nº 12.527/2011), que regulou o acesso a dados, inclusive pessoais, para fins de transparência na gestão pública. O artigo 4º, I, conceitua **informação** como "dados, processados ou não, que podem ser utilizados para produção e

transmissão de conhecimento, contidos em qualquer meio, suporte ou formato". Embora a lei não veicule a expressão "dados pessoais", é utilizado um conceito conjugado de dados pessoais com informação, que engloba a ideia de dados pessoais.[9]

O artigo 4º, IV, define **informação pessoal** como "aquela relacionada à pessoa natural identificada ou identificável", muito se aproximando do conceito de dados pessoais da LGPD (artigo 5º, I, da LGPD).

Com isso, a LAI começa a delinear um conjunto de direitos a fim de resguardar a informação pessoal. Já no artigo 6º, III, fica definido que os órgãos e entidades do poder público devem assegurar a "proteção da informação sigilosa e da informação pessoal, observada a sua disponibilidade, autenticidade, integridade e eventual restrição de acesso".

Nesse diapasão, a informação sigilosa e a informação pessoal são equiparadas no que se refere a medidas de **segurança da informação**, visto que os conceitos inscritos se relacionam justamente a essa seara do conhecimento. Conforme prescreve HINTZBERGEN *et al.* (2018, p. 21 e p. 27), "[c]onfidencialidade, integridade e disponibilidade são princípios críticos de segurança da informação", acrescentando que os atributos do hexagrama Parkeriano são confidencialidade, posse ou controle, integridade, autenticidade, disponibilidade e utilidade.

Quanto à segurança da informação, alguns setores, como o bancário e o de mercado de capitais, possuem regulamentações mais específicas sobre segurança cibernética, como a Resolução nº 4.658, de 26 de abril de 2018, do Banco Central do Brasil, posteriormente revogada pela Resolução nº 4.893, de 26 de fevereiro de 2021, e a Instrução CVM nº 612, de 21 de agosto de 2019, que alterou profundamente a Instrução CVM nº 505, de 27 de setembro de 2011.

Em setores desregulamentados, o direito brasileiro deixa espaços para a aplicabilidade de normas privadas, já que não há uma lei que trate do tema para as empresas privadas. Nesse contexto, despontam as normas da *International Organization for Standardization* – ISO sobre o tema:

---

[9] Segundo MICHAELIS (2021), **dados** são "Informações que identificam o indivíduo". **Informação**, por sua vez, é o "conjunto de conhecimentos acumulados sobre certo tema por meio de pesquisa ou instrução" ou "explicação ou esclarecimento de um conhecimento, produto ou juízo; comunicação".

> Os objetivos das normas 27001 e 27002 são distintos entre si. A **norma 27001:2006** especifica os requisitos para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um SGSI documentado dentro do contexto dos riscos de negócio globais da organização. Ela especifica requisitos para a implementação de controles de segurança personalizados para as necessidades individuais de organizações ou suas partes. Segundo essa norma, a implementação do SGSI é baseada no esquema PDCA (Plan-Do-Check-Act), amplamente utilizado na administração.
>
> Já a **norma 27002:2005** estabelece diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão de segurança da informação em uma organização. Os objetivos definidos nesta norma provêem diretrizes gerais sobre as metas geralmente aceitas para a gestão da segurança da informação. (TEIXEIRA FILHO, 2015, pp. 3-4)

Além das normas ISO, ROCHA (2020, p. 221) destaca outras associações e órgãos que se debruçam sobre o tema no Brasil e no mundo, como o *National Institute of Standards and Technology – NIST* (EUA), a *European Union Agency for Cybersecurity – ENISA*, o *Open Web Application Security Project – OWASP*, e o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil – CERT.br.

Diferentemente do Brasil com a LGPD, o GDPR abraçou algumas das normativas internacionais e ressaltou, de maneira mais enfática, as questões relativas à segurança da informação. Esse conjunto de salvaguardas tecnológicas trazidas no GDPR será importante para, por exemplo, dar concretização aos ditames da LGPD, conforme será tratado mais adiante. Consoante descreve MARINHO (2020, p. 64):

> Como já visto anteriormente, encontraremos ao longo do GDPR a indicação de oito itens da Norma ISO 27001 (segurança da informação):
>
> - Política de segurança;
> - Classificação de informação;
> - Controle de acesso;
> - Pentest (teste de invasão);
> - Gestão formal (documentada) de backup;
> - Criptografia;

- Plano de Continuidade de Negócios (PCN/BCP);
- Plano de Resposta a Incidentes.

Quanto ao conceito de incidente de segurança, constantemente trazido nas normas de segurança da informação, convém destacar a definição técnica abaixo:

> Um incidente de segurança da informação é indicado por um único ou uma série de eventos de segurança da informação, indesejáveis ou inesperados, que tenham uma probabilidade significativa de comprometer a operação dos negócios e ameacem a segurança da informação. (HINTZBERGEN *et al.*, 2018, p. 14)

As normas de proteção de dados têm ventilado, portanto, questões de segurança da informação em seu bojo – tal como ocorre na LAI. Como exemplo, pode-se observar tal fenômeno no tratamento jurídico sobre o acesso às informações pessoais.

A Seção V da LAI trata exclusivamente das informações pessoais. O *caput* do artigo 31, por sua vez, resgata os princípios em relação ao tratamento dessas informações:

> Art. 31. O tratamento das informações pessoais deve ser feito de forma transparente e com respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais

Nota-se que o artigo 31 resgata o conteúdo constitucional de preservação à privacidade dos indivíduos. E o parágrafo primeiro reforça que as informações com potencial de violação à intimidade, vida privada, honra e imagem:

> I – terão seu acesso restrito, independentemente de classificação de sigilo e pelo prazo máximo de 100 (cem) anos a contar da sua data de produção, a agentes públicos legalmente autorizados e à pessoa a que elas se referirem; e

> II – poderão ter autorizada sua divulgação ou acesso por terceiros diante de previsão legal ou consentimento expresso da pessoa a que elas se referirem.

Ou seja, automaticamente, as informações pessoais exibem restrições de acesso como medida de segurança da informação, somente sendo possível o acesso a agentes públicos legalmente autorizados e ao próprio interessado. A exceção (divulgação ou acesso a terceiros) dependerá de consentimento expresso[10] da pessoa envolvida, ou então de previsão legal que autorize esse uso compartilhado.

Uma medida técnica e considerada uma boa prática para restrição de acesso é a manutenção dos *logs* das operações de tratamento que envolvam dados pessoais, conforme destacado a seguir, ajudando a garantir a efetividade da regra descrita no parágrafo anterior:

> Assim, deve ser mantido o registro (log) de execução dos tratamentos, sejam automáticos ou manuais.
>
> A execução deste controle implica a evidenciação dos registros (logs) de execução dos tratamentos. (GARCIA *et al.*, 2020, p. 75)

E, para o controle desses *logs*, é importante se realizar um gerenciamento específico de modo a permitir uma melhor análise dos acessos realizados e verificar eventuais abusos:

---

[10] Quando exigem consentimento **expresso**, as normas deixam evidente a necessidade de um comportamento ativo por parte do titular de dados, o que não se confunde com o consentimento **tácito**. TARTUCE (2021, p. 225) prescreve que: "O consentimento pode ser *expresso* – escrito ou verbal, no primeiro caso de forma pública ou particular –, ou *tácito* – quando resulta de um comportamento implícito do negociante, que importe em concordância ou anuência. Nesse sentido, preconiza o art. 111 do CC/2002 que o silêncio importa anuência, quando as circunstâncias ou os usos o autorizarem, e não for necessária a declaração de vontade expressa. Desse modo, por regra, quem cala não consente, eis que, para que seja válida a vontade tácita, devem estar preenchidos os requisitos apontados." (grifos do original).

> [...] Uma solução de gerenciamento de **logs** (**log management**) permite **centralizar e consolidar os logs** em um único local para fins de análise e armazenamento. As funções primordiais de um gerenciador de **logs** são:
>
> - coletar e armazenar volumes massivos de dados;
> - processar e normalizar **logs** de diversas fontes;
> - armazenar e reter **logs** para longo prazo;
> - proteger os dados do registro de eventos contra adulteração ou destruição;
> - criar relatório de **log**;
> - analisar **logs**. (DONDA, 2020, p. 79)

Alguns países contam com um controle robusto de acesso a dados pessoais por servidores públicos justamente para evitar acessos não autorizados, considerando que pessoas possam se valer de uma eventual posição privilegiada para obter vantagens ilícitas. Logo, esse importante princípio de segurança, além das normas ISO, vem sendo exigido do setor público:

> Como medida de segurança da informação, um exemplo é o sistema de registro automático de acesso às atividades relacionadas aos dados de seus cidadãos da Estônia. O registro permite consultar quem acessou os dados, identificando qualquer acesso indevido ou desnecessário, possibilitando a denúncia à invasão de privacidade. Essa medida levou à responsabilização de funcionários públicos que acessaram dados privados sem autorização ou necessidade funcional. (SERAFINO, 2020, p. 255)

No Brasil, com o advento da LGPD, tiveram início as preocupações de algumas autoridades[11] fazendárias para justamente limitar o acesso às informações de arquivos para somente pessoas autorizadas fazerem uso das respectivas informações. Isso porque o tratamento para fins tributários precisa ser bem tutelado para não correr o risco de violações com os objetivos de tratamento, em especial o uso dessas informações para outras finalidades:

[11] Utilizaremos a expressão “autoridade tributária” como “administração tributária”.

> [...] Motivados pela promulgação da LGPD, os sistemas da SEFAZ e da CONFAZ alteraram a forma de consultas das informações dos arquivos XML, visando garantir que apenas as pessoas autorizadas pudessem visualizar os documentos. (SERAFINO, 2020, p. 253)

O artigo 31, § 2º, por sua vez, resguarda a responsabilização em caso de uso indevido, imprimindo mais uma garantia de segurança a esses dados ao deixar evidente que a força da lei recairá sobre quem violar tais restrições. Já o artigo 34 impõe a responsabilidade ao órgão ou entidade, devendo fazer a apuração funcional nos casos de dolo ou culpa, assegurado o direito de regresso.

O artigo 116 da Lei nº 8.112/1990, inciso VIII, coloca como dever do servidor público federal a guarda de sigilo sobre assunto de sua repartição, além de prestar as informações requeridas pelo público, ressalvadas as protegidas por sigilo (inciso V, alínea “a”, do mesmo artigo). Em caso de descumprimento, isso poderá ensejar a instauração de Processo Administrativo Disciplinar – PAD.

Ademais, cumpre salientar que o artigo 154 do Código Penal tipifica a conduta de violação do segredo profissional como crime, quando o autor revela a alguém, sem justa causa, segredo em razão da função e cuja revelação cause danos a outrem.

Por conseguinte, o agente responde na medida de sua culpabilidade, enquanto o órgão ou entidade responde na modalidade do artigo 37, § 6º, da Constituição da República Federativa do Brasil, ou seja, de maneira objetiva, podendo acionar o agente público infrator com base no direito de regresso.

No que se refere ao consentimento do titular, ele não será exigido quando as informações forem necessárias, conforme artigo 31, § 3º:

> I – à prevenção e diagnóstico médico, quando a pessoa estiver física ou legalmente incapaz, e para utilização única e exclusivamente para o tratamento médico;
>
> II – à realização de estatísticas e pesquisas científicas de evidente interesse público ou geral, previstos em lei, sendo vedada a identificação da pessoa a que as informações se referirem;
>
> III – ao cumprimento de ordem judicial;

> IV – à defesa de direitos humanos; ou
>
> V – à proteção do interesse público e geral preponderante.

Com fundamento na restrição de acesso à informação, o artigo 31, § 4º, prescreve que:

> A restrição de acesso à informação relativa à vida privada, honra e imagem de pessoa não poderá ser invocada com o intuito de prejudicar processo de apuração de irregularidades em que o titular das informações estiver envolvido, bem como em ações voltadas para a recuperação de fatos históricos de maior relevância.

Como se percebe, embora seja um princípio de direito constitucional, não se trata de algo absoluto, comportando a dispensa do consentimento em casos nos quais o sopesamento de princípios impõe a aplicação de outro valor, como a dignidade da pessoa humana, o interesse público, o devido processo legal e a ampla defesa ou o patrimônio histórico e cultural, por exemplo. WIMMER (2021, p. 280 e p. 284) ressalta, porém, que o consentimento, quando envolve relações público-privadas, é visto com desconfiança porque há uma posição desigual na relação entre Estado e indivíduo.

O debate mais recente refere-se à falta de harmonização da linguagem e das medidas técnicas desde o advento da LAI e que se agravou com a LGPD, conforme pontua WIMMER (2021, p. 276). Ademais, some-se a isso o fato de a LGPD ser uma lei que carece de técnica legislativa apurada, conforme se verá mais adiante.

1.2.2. Marco Civil da Internet – MCI (Lei nº 12.965/2014)

Embora a LAI tenha disciplinado diversas questões atinentes a dados pessoais, como se depreendeu do item anterior, havia a necessidade de um marco

normativo que trouxesse a tutela ao principal meio de tratamento de dados pessoais da atualidade: a internet. Com o Marco Civil da Internet – MCI (Lei nº 12.965/2014), o artigo 3º, III, estabeleceu que a disciplina do uso da internet no Brasil tem, como princípio, a proteção de dados pessoais na forma da lei. É o prenúncio de uma disciplina infraconstitucional que seja mais específica para a proteção de dados pessoais e mais centrada no indivíduo – considerando que a LAI, precipuamente, é mais voltada à transparência e ao interesse público.

O MCI regula disposições específicas sobre dados pessoais, como no artigo 7º, no qual fica consignado que o acesso à internet é essencial ao exercício da cidadania, garantindo os direitos aos usuários:

> **(i) não fornecimento a terceiros** de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei (inciso VII);
>
> **(ii) informações claras e completas** sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que (inciso VIII):
>
> a) justifiquem sua coleta;
> b) não sejam vedadas pela legislação; e
> c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet;
>
> **(iii) consentimento expresso** sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais (inciso IX);

> **(iv) exclusão definitiva** dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei (inciso X), sendo vedada, nas aplicações de internet, a guarda de dados pessoais que sejam excessivos em relação à finalidade para a qual foi dado consentimento pelo seu titular (art. 16, II)[12].

Ficou também insculpido no artigo 9º o princípio de neutralidade da rede, com o dever de tratamento isonômico em relação aos pacotes de dados, não havendo distinção por conteúdo, origem e destino, serviço, terminal ou aplicação.

Além desses direitos aos usuários (alguns muito similares ao que constam no artigo 18 da LGPD), a Seção II do MCI veicula a proteção aos registros, aos dados pessoais e às comunicações privadas. Nesse sentido, o art. 10 resguarda expressamente a preservação da intimidade, da vida privada, da honra e da imagem das partes. O parágrafo primeiro exige que os provedores somente forneçam os respectivos registros necessários para identificar o indivíduo mediante ordem judicial, elevando o *status* da proteção dos indivíduos, considerando que não é possível romper a privacidade por meios extrajudiciais.

O parágrafo terceiro ressalva, no entanto, que as autoridades administrativas com competência legal podem ter acesso a dados cadastrais "que informem qualificação pessoal, filiação e endereço".

Além disso, o artigo 11 consigna expressamente que:

> Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à

[12] Não é despiciendo ressaltar que esses direitos foram introduzidos posteriormente pela LGPD, alterando o MCI.

> privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros.

Isso já representa um prelúdio ao conteúdo da LGPD, que vai justamente na direção de disciplinar esses tópicos no que se refere à territorialidade da lei (ampliando também em relação à extraterritorialidade). O artigo 11, § 1º, consigna que o comando do *caput* "[a]plica-se aos dados coletados em território nacional e ao conteúdo das comunicações, desde que pelo menos um dos terminais esteja localizado no Brasil".

O MCI também começou a pavimentar o caminho para a interoperabilidade e acessibilidade em relação à base de dados, homenageando os padrões tecnológicos abertos que costumam ser a regra no setor público. Esse é o conteúdo do artigo 4º, inciso IV.

Esses conceitos serão importantes para a LGPD e sua aplicação no setor público, visto que há uma ênfase à interoperabilidade e acessibilidade de base de dados entre os órgãos e entidades públicas. No artigo 25 da LGPD, por exemplo, há a ressalva de que os dados sejam mantidos em formato interoperável e estruturado[13] para o uso compartilhado.

No que se refere ao setor público, o artigo 24 do MCI consigna que as diretrizes para atuação dos entes federativos estão em direção à "publicidade e disseminação de dados e informações públicos, de forma aberta e estruturada" (inciso VI) e "otimização da infraestrutura das redes e estímulo à implantação de centros de armazenamento, gerenciamento e disseminação de dados no País [...]" (inciso VII). O MCI, no entanto, mantém a disciplina da atuação no setor público no que se refere a base de dados, na linha evolutiva inaugurada pela LAI.

Outrossim, vale a pena destacar a recente Lei nº 14.129/2021, a qual dispõe sobre princípios, regras e instrumentos para o Governo Digital e para o aumento da eficiência pública, cujo Capítulo IV, Seção II, trata da interoperabilidade de dados entre órgãos públicos.

[13] Com relação ao conceito de dados estruturados, ver item 1.3.5.

1.3. Lei Geral de Proteção de Dados Pessoais – LGPD (Lei nº 13.709/2018) e suas diversas atecnias

Conforme destacado anteriormente, a LGPD surgiu, sobretudo, em resposta aos escândalos veiculados envolvendo a *Cambridge Analytica* e as eleições presidenciais de 2016 nos Estados Unidos da América, bem como o resultado do Brexit. Trata-se de uma resposta ao uso indiscriminado de dados pessoais na internet para fins econômicos, sobretudo nas redes sociais como Facebook, Instagram e Twitter, e em observância ao movimento ocorrido na Europa com a entrada em vigor do GDPR em 2018.

O Projeto de Lei nº 4.060/2012 da Câmara dos Deputados, de autoria do Deputado Federal Milton Monti (PR/SP), foi a gênese da atual LGPD. Posteriormente, o Deputado Federal Orlando Silva (PCdoB/SP) serviu como relator para a redação final da Lei nº 13.709/2018, promulgada em 14 de agosto de 2018 e publicada no dia seguinte.

Na Justificativa do PL, o Deputado expõe que:

> O tratamento de dados é hoje uma realidade cada vez mais presente em nosso cotidiano, especialmente quando experimentamos o avanço da tecnologia da informação, em especial a internet e suas aplicações nas mais diversas áreas de nossa vida em sociedade. Até pouco tempo era inimaginável pensar nas aplicações e a interação que a internet teria em nosso dia-a-dia, ao mesmo tempo em que podemos imaginar que isso continuará em ritmo acelerado e de incremento, tendo em vista a velocidade em que novas tecnologias são desenvolvidas para a comunicação com as pessoas.
>
> Dentro dessa realidade se faz necessário estabelecer normas legais para disciplinar tais relações, especialmente para dar proteção à individualidade e a privacidade das pessoas, sem impedir a livre iniciativa comercial e de comunicação.

Portanto, a importância de uma disciplina jurídica específica da matéria é bastante explicitada no PL, sobretudo pelos motivos de evolução tecnológica que já foram abordados alhures. Embora tenha sido objeto de amplos debates

legislativos, o resultado dos debates que originaram a LGPD foi de uma lei deficiente em alguns aspectos técnicos. O uso de conceitos jurídicos indeterminados, redundantes e de maneira atécnica faz com que recaia sobre a LGPD muitas dúvidas interpretativas que dificultam a aplicação do exegeta, bem como do operador do Direito. Isso afeta tanto os aspectos de direito privado como os de direito público.

A prolixidade da LGPD também a denota como uma lei que não apresenta muita assertividade ao gerar obrigações às pessoas naturais e jurídicas, em especial no tocante ao setor público. Ou seja, soa como uma lei na defensiva contra potenciais ataques jurídicos que porventura possam surgir, e por esse motivo delineia, de maneira até um pouco exagerada, pontos que são mais procedimentais do que normativos.

Uma sugestão seria que a LGPD pudesse ser, em breve, revista e republicada, observando a terminologia correta da legística nacional, para assim evitar dúvidas interpretativas que certamente surgirão. Melhor dizendo, ainda que pareça prematuro, a LGPD já nasce com a necessidade de uma verdadeira reforma – mesmo tendo sido uma lei que já foi alterada em diversas oportunidades, como será visto a seguir.

1.3.1. Polêmica em relação ao início de sua vigência

Uma questão controversa que surgiu desde o início do processo da LGPD foi a definição de sua data de vigência. O texto original prescrevia, no artigo 65, que a lei entraria em vigor dezoito meses depois de sua publicação oficial. Como foi sancionada em 14 de agosto de 2018 e publicada em 15 de agosto de 2018, ela deveria entrar em vigor no dia 16 de fevereiro de 2020 – nos termos do artigo 8º, § 1º, da Lei Complementar nº 95/1998.[14]

[14] Art. 8º A vigência da lei será indicada de forma expressa e de modo a contemplar prazo razoável para que dela se tenha amplo conhecimento, reservada a cláusula “entra em vigor na data de sua publicação” para as leis de pequena repercussão.

Tratava-se de um prazo muito otimista e inferior à *vacatio legis* do GDPR, de dois anos, visto que a norma foi promulgada em 27 de abril de 2016 e entrou em vigor em 25 de maio de 2018 (artigo 99º, item 2, do GDPR).

Talvez mirando algum ajuste mais consentâneo à realidade econômica para a adaptação a uma norma com esta envergadura, com a edição da Medida Provisória nº 869, de 2018, a data de entrada em vigor foi estendida, por meio da criação do inciso II, para 24 meses após a data da publicação em relação aos artigos que não se referiam à estrutura da Autoridade Nacional de Proteção de Dados Pessoais – ANPD.[15] Essas novas datas foram confirmadas pela conversão da referida Medida Provisória na Lei nº 13.853/2019.

Nesse contexto, *ceteris paribus,* a LGPD passaria a entrar em vigor, com a nova alteração legal, no dia 16 de agosto de 2020. No entanto, em virtude do advento da pandemia da Covid-19 no final de 2019, em abril de 2020 foi publicada a Medida Provisória nº 959/2020, a qual estendia novamente o prazo de entrada em vigor da LGPD para 3 de maio de 2021.

Paralelamente, em junho de 2020, foi publicada a Lei nº 14.010/2020, a qual dispôs sobre o Regime Jurídico Emergencial e Transitório das Relações Jurídicas de Direito Privado – RJET no período da pandemia do coronavírus, fruto do Projeto de Lei do Senado Federal (PLS) nº 1.179/2020 do Senador Antonio Anastasia (PSD/MG). Houve a inclusão do inciso I-A no artigo 65, para que a vigência das sanções administrativas a serem aplicadas pela ANPD passasse a ser a partir de 1º de agosto de 2021. Ato contínuo, a entrada em vigor da LGPD, com relação aos demais dispositivos, permaneceria a data de 16 de agosto de 2020.

No entanto, como a MP alterava essa sistemática, foi necessário que o Congresso se debruçasse repetidamente sobre o tema na mesma sessão legislativa. Na tramitação para a conversão dessa Medida Provisória em lei, o Congresso Nacional chegou a apresentar uma redação alternativa, sugerindo que a LGPD pudesse entrar em vigor em 31 de dezembro de 2020. Ocorre que, quando encaminhada ao Senado, o então Presidente Davi Alcolumbre (DEM/AP) não levou

---

§ 1º A contagem do prazo para entrada em vigor das leis que estabeleçam período de vacância far-se-á com a inclusão da data da publicação e do último dia do prazo, entrando em vigor no dia subseqüente à sua consumação integral.

[15] Segundo o inciso I, quanto aos art. 55-A, 55-B, 55-C, 55-D, 55-E, 55-F, 55-G, 55-H, 55-I, 55-J, 55-K, 58-A e 58-B, entrariam em vigor no dia 28 de dezembro de 2018.

o referido tópico da nova vigência da LGPD para votação, mas somente os demais dispositivos que a MP tratava, com a argumentação de que o tema já havia sido apreciado quando da discussão do PLS nº 1.179/2020. Com essa decisão, a sugestão de emenda feita pela Câmara dos Deputados perdeu o efeito, bem como o prazo de 3 de maio de 2021 estatuído pela Medida Provisória.

Com o envio para a sanção presidencial da referida MP, a qual veio a se tornar a Lei nº 14.058/2020, o novel inciso II perdeu efeito, e o inciso original da norma foi restaurado para o prazo anterior de 24 meses para a entrada em vigor. Como a sanção presidencial se deu somente em 17 de setembro de 2020 e a publicação da lei ocorreu no dia seguinte, a LGPD passou a vigorar, oficialmente, em 18 de setembro de 2020.

Pode-se discutir se a lei teria o condão de operar uma espécie de repristinação e entrar em vigor de maneira retroativa, para que a data original dos 24 meses de *vacatio legis* fosse observada – nesse sentido, ela entraria em vigor no mês anterior, em 16 de agosto de 2020. No entanto, entendemos que isso geraria insegurança jurídica e feriria atos jurídicos perfeitos praticados sob a égide da Medida Provisória nº 959/2020: as operações de tratamento de dados pessoais feitas nesse período, até o dia 18 de setembro, estariam alcançadas por essa espécie de repristinação do inciso anterior, de modo que essa seria a melhor interpretação em relação a esse período de entrada em vigor.[16]

Portanto, a fim de que as empresas tenham a segurança jurídica da data a partir da qual estão sujeitas à LGPD, a interpretação majoritária e mais razoável é que a data de entrada em vigor da lei ficou fixada em 18 de setembro de 2020.

1.3.2. Veto à criação da ANPD

Outra polêmica que despontou em relação à LGPD foi a de que a lei teria sido publicada com todos os dispositivos relativos à entidade que fiscalizaria seu cumprimento vetados pela Presidência da República. Os artigos 55 ao 59 foram

[16] Essa, inclusive, é a interpretação do SENADO FEDERAL (2020).

vetados porque “incorrem em inconstitucionalidade do processo legislativo, por afronta ao artigo 61, § 1º, II, ‘e’, cumulado com o artigo 37, XIX da Constituição”, conforme disposto na Mensagem de Veto Presidencial nº 451, de 14 de agosto de 2018. De fato, tendo o projeto de lei sido de autoria do Poder Legislativo, não haveria como criar órgãos da administração pública dentro do Poder Executivo ou aumentar despesas. Essa iniciativa caberia à Presidência da República, e o veto, sob o ponto de vista jurídico, está correto.

Portanto, meses depois, foi promulgada pelo Poder Executivo a Medida Provisória nº 869, de 27 de dezembro de 2018, assinada pelo então presidente Michel Temer, a qual fixaria esse vício legislativo. Posteriormente ela foi convertida na Lei nº 13.853/2019, alterando este e outros pontos substanciais da LGPD.

Cumpre salientar que, nesse ponto, entendemos que o mais adequado seria ter havido o envio de projeto de lei de autoria do Poder Executivo com esse teor, para que pudesse ser debatido no Parlamento dentro do processo legislativo comum, haja vista que a referida Medida Provisória não preencheria adequadamente os requisitos de relevância e urgência do artigo 62 da Constituição da República Federativa do Brasil.

A maior prova fática disso é que a ANPD foi formalmente estruturada somente em agosto de 2020 com o Decreto nº 10.474/2020, portanto, mais de dois anos depois de sua publicação.[17] Logo, o período de dois anos seria mais do que suficiente para que as duas Casas do Congresso Nacional apreciassem a criação da ANPD, bastando que houvesse vontade política e organização legislativa para tanto. O uso da Medida Provisória mostrou-se via legislativa inadequada para a finalidade pretendida.

1.3.3. Conteúdo prolixo e atecnias no texto legislativo

[17] Em virtude da celeuma narrada nos parágrafos anteriores.

Não foi somente o prazo de entrada em vigor ou a não criação da ANPD que transformou a LGPD em uma celeuma jurídica. Outras controvérsias também erigem em relação à temática.

Trata-se de uma lei também bastante criticada pela doutrina: pouco em razão de seu conteúdo material (aguardado e festejado pelos profissionais da área de privacidade e proteção de dados pessoais), mas muito em razão de sua redação com inobservância a algumas questões formais. Conforme expõe a doutrina mais abalizada:

> Todavia, a técnica legislativa utilizada no caso brasileiro, cuja boa intenção não se questiona, parece-nos conducente a certos impasses. Cuida-se, com efeito, de um texto prolixo, explicitando referências principiológicas generalizantes, mas que não raro levam a direções divergentes; contendo amplo rol de proibições aparentemente severas, no entanto logo seguidas de amplas exceções; apresentando um regime de pesada responsabilização, por violações da Lei que nem sempre serão claramente caracterizáveis; e, para culminar, estabelecendo uma governança do sistema atribuída a uma autoridade administrativa com poderes não nitidamente delimitados, em especial no ambiente federativo, competente para fixar padrões de interpretação de uma Lei repleta de porosidades. (ALMEIDA; LINO, 2020, p. 328)

De fato, uma análise mais acurada da LGPD permite a extração de diversos pontos controversos em relação ao seu texto. Não se questiona, aqui, o trabalho de legística do Congresso Nacional, que é de alta qualidade. Porém, como é uma lei que é resultado de aportes de vários setores da sociedade, é natural que ela acabe veiculando atecnias na sua redação final.

Talvez a primeira observação seja o uso do termo “Geral”, inspirado diretamente no GDPR, e que era utilizado de maneira informal pela doutrina até a sua positivação pela Lei nº 13.853/2019, que inseriu a expressão “Lei Geral de Proteção de Dados Pessoais (LGPD)” na ementa da Lei nº 13.709/2018. No entanto, na União Europeia, a terminologia “geral” imprime o sentido de que a norma é autoaplicável a todos os 27 Estados-Membros, sem necessidade de disciplina legislativa local, como já detalhamos anteriormente.

Entretanto, no caso brasileiro, a norma é de interesse nacional, o que é reforçado no parágrafo único do art. 1º, sendo aplicável à União, Estados, Distrito

Federal e Municípios. O referido dispositivo foi incluído pela Lei nº 13.853/2019, resultado da conversão da Medida Provisória nº 869, de 2018, trazendo maior claridade em relação à sua aplicabilidade nacional.

Nesse sentido, o "Geral" não traz contribuições substanciais à terminologia da lei, pois seria o equivalente a denominar o Código Tributário Nacional de "Código Geral Tributário". Em verdade, poucas leis brasileiras utilizam o termo "Geral" em sua denominação justamente por ser um vocábulo que empresta um conteúdo jurídico específico no contexto brasileiro federativo. Como exemplo, pode-se citar a Lei Geral de Telecomunicações (Lei nº 9.472/1997), embora não seja a denominação oficial da ementa da lei como no caso da LGPD.

No contexto de competências constitucionais, a terminologia "geral" remete ao conteúdo do artigo 24 da Constituição da República Federativa do Brasil, que trata das competências concorrentes. No § 1º do indigitado dispositivo, fica consignado que a União estabelecerá "normas gerais", cabendo aos estados a "competência suplementar" (§ 2º). Portanto, não é possível afirmar que o "geral" se refere à competência da União para editar normas gerais, conforme prescreve o artigo 24, § 1º, da Constituição da República Federativa do Brasil, visto que não há, nesse dispositivo, qualquer menção à possibilidade de legislar sobre proteção de dados pessoais.

Mais consonante à nossa formação federativa seria, portanto, que a nomenclatura representasse a expressão "Lei Nacional de Proteção de Dados Pessoais – LNPD", até mesmo para se diferenciar de outras normas locais sobre a mesma temática, como ocorre com o CCPA nos Estados Unidos.

Outro ponto é a forma como a LGPD se refere às estruturas de direito público, demonstrando um desconhecimento da terminologia consagrada na ciência do Direito Administrativo e do Direito Tributário. ALVES (2020a, p. 178), ao tratar do uso plurívoco de termos para se referir às estruturas da Administração Pública, imprime uma crítica à redação da LGPD, que seria desprovida das obrigações legísticas trazidas pelo ordenamento nacional: "[o] ideal teria sido uma redação mais precisa e detalhada na LGPD, até mesmo em respeito à Lei Complementar nº 95, de 1998".

Como ALVES (2020a, p. 178) demonstra, são utilizadas expressões como **poder público** (em minúsculo e maiúsculo), **entidade pública**, **ente público**,

órgão público, tudo sem seguir os critérios rígidos do Decreto-Lei nº 200/1967 e da Lei nº 9.784/1999, a Lei de Processo Administrativo Federal. Isso dificulta, sobretudo, na aplicabilidade da LGPD às relações de direito público, causando diversas dúvidas aos operadores do Direito.

Para a Lei nº 9.784/1999, órgão é "a unidade de atuação integrante da estrutura da Administração direta e da estrutura da Administração indireta" e entidade é "a unidade de atuação dotada de personalidade jurídica" (artigo 1º, § 2º, I e II, respectivamente). O ente seria ligado ao conceito de federação (União, Estados, Distrito Federal e Municípios), conforme definição no artigo 2º, inciso I, da Lei Complementar nº 101/2000, a Lei de Responsabilidade Fiscal.

Outra confusão advém do conceito de uso compartilhado de dados, inscrito no artigo 5º, inciso XVI. Segundo o indigitado dispositivo:

> XVI – uso compartilhado de dados: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados;

Com relação ao conteúdo deste dispositivo, detalha WIMMER (2021, p. 282):

> Por outro lado, cumpre registrar que a LGPD tratou de maneira pouco sistemática das condições objetivas para o compartilhamento de dados pessoais custodiados pelo Poder Público, a começar pela definição de "uso compartilhado". O art. 5.º, XVI, indica que o conceito pode ser utilizado para se referir ao compartilhamento de dados em três contextos: (i) entre órgãos e entidades públicos; (ii) entre órgãos e entidades públicos e entes privados, "com autorização específica"; ou (iii) entre entes privados.

Em relação a essa problemático, o primeiro tópico a se destacar é a ausência da qualificadora "pessoais" junto ao substantivo "dados" – um conceito

muito abrangente que poderia englobar também dados empresariais. O segundo é que a LGPD, por vezes, abandona o uso da definição, utilizando termos que geram dúvidas, como “compartilhar dados pessoais” (artigo 7º, § 5º), cujo verbo não está contido no conceito supramencionado (afinal, a definição é de “uso compartilhado”, e não “compartilhar”).

Também não está inscrita a expressão “compartilhamento” nas vinte espécies do conceito de tratamento, também descrito no artigo 5º, inciso X:

> X – tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

Como se pode depreender, não há menção ao substantivo “compartilhamento” na qualidade de espécie de tratamento. Logo, somente podemos considerar como expressão legalmente definida a “uso compartilhado”. Ou seja, ao tratar de compartilhamento, a LGPD usa essa expressão como sinônima de forma atécnica. Isso porque o uso compartilhado é para a relação público-privada ou público-pública, não podendo ser usada tal definição para a disciplina privada-privada – como no caso de tratamento de dados pessoais envolvendo co-controladores, por exemplo.

Essa atecnia não ocorre somente no uso da expressão “compartilhar dados pessoais”, mas também no “tratamento compartilhado”, conforme consta no artigo 11, inciso II, alínea “b”. O artigo 11 disciplina o regime de tratamento de dados pessoais sensíveis, e, exceto por pequenas diferenças, muito se assemelha ao artigo 7º, que rege o tratamento de dados pessoais de maneira geral.

No entanto, a regra “espelho” contida no artigo 7º, inciso III, utiliza-se corretamente da expressão “tratamento **e uso compartilhado de dados**”, mantendo, desse modo, a aderência às definições do artigo 5º da LGPD. Isso só reforça a falta de padronização dos conceitos e terminologia dessa lei.

Percebe-se, portanto, que a LGPD definiu a expressão “uso compartilhado”, mas também admite outros vocábulos com esse sentido, embora não estejam definidos na lei, tais como “compartilhar” e “compartilhamento” – este último, embora não esteja previsto na LGPD, é amplamente usado na práxis de proteção de dados e privacidade.

A LGPD também é prolixa no artigo 3º, ao definir sua aplicação territorial e extraterritorial. O inciso I é muito parecido com o III, visto que aquele prescreve que a lei é aplicável desde que “a operação de tratamento seja realizada no território nacional”, ao passo que este detalha a menos que “os dados pessoais objeto do tratamento tenham sido coletados no território nacional”. Ora, considerando que coleta é uma espécie do gênero “tratamento”, o inciso III já estaria contido na ideia do inciso I, levando a uma certa redundância.

Outro ponto de controvérsia semântica é o artigo 7º, inciso V, que delineia a hipótese de tratamento de dados pessoais “quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados”.

Por essa redação, o aposto “a pedido do titular dos dados” aparentemente se refere às duas hipóteses, que são execução de contrato ou procedimento preliminar relacionado a contrato. Ocorre que, na redação do GDPR, com uma clareza solar muito maior, o artigo 6º, item 1, “b”, delineia que o tratamento é lícito quando “[...] for necessário para a execução de um contrato no qual o titular dos dados é parte, ou para diligências pré-contratuais a pedido do titular dos dados”.

Assim, percebe-se que, no GDPR, não há dúvidas de que são duas situações distintas em que o tratamento é permitido: execução de contrato e diligências pré-contratuais a pedido do titular. Logo, o pedido do titular só é necessário quando for relativo à diligência pré-contratual.

Já na LGPD, o mencionado dispositivo deixa dúvidas, pois caberia a interpretação de que é exigido o pedido do titular tanto para execução de contrato como para procedimentos preliminares. Considerando que a LGPD se inspirou, ainda que de maneira precária, no GDPR, entendemos que a interpretação a ser dada a esse dispositivo, em sede administrativa e judicial, será na linha do que é definido no GDPR, a saber: independe do pedido do titular caso o controlador trate dados pessoais para a finalidade de execução do objeto de um contrato.

Outro tema que merece destaque é a falta de conexão no momento de disciplinar temas que deveriam estar mais concatenados, podendo também ensejar confusão ao exegeta. A LGPD disciplina, em seu artigo 16, sobre a eliminação de dados pessoais, autorizando a conservação para as seguintes finalidades:

> Art. 16. Os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades:
>
> I – cumprimento de obrigação legal ou regulatória pelo controlador;
>
> II – estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
>
> III – transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou
>
> IV – uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.

Logo, entende-se que qualquer conservação de dados que não esteja em conformidade com essas quatro situações seria indevida e desnecessária, portanto, em desconformidade com a LGPD. O titular de dados poderia ainda solicitar a eliminação desses dados, com base no artigo 18, inciso IV: “anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei”.

Todavia, como se depreende, o controlador teria o dever de **eliminar** os dados, e o titular poderia solicitar **anonimização** ou **bloqueio**, alternativamente à eliminação. Vale ressaltar que isso representa uma maior obrigação ao controlador, que deverá estar dotado de ferramentas técnicas para realizar tanto a anonimização quanto o bloqueio, medidas muito mais complexas que a simples eliminação.

A título de exemplo, cumpre mencionar o Considerando nº 67 do GDPR, que traz exemplos mais próximos do conceito de bloqueio da LGPD (artigo 5º, XIII). Nesse dispositivo, a LGPD prescreve que bloqueio é a “suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco

de dados". Como não há exemplos de aplicação dessa técnica, recorre-se ao Considerando supramencionado:

> Para restringir o tratamento de dados pessoais pode recorrer-se a métodos como a transferência temporária de determinados dados para outro sistema de tratamento, a indisponibilização do acesso a determinados dados pessoais por parte dos utilizadores, ou a retirada temporária de um sítio web dos dados aí publicados. Nos ficheiros automatizados, as restrições ao tratamento deverão, em princípio, ser impostas por meios técnicos de modo a que os dados pessoais não sejam sujeitos a outras operações de tratamento e não possam ser alterados. Deverá indicar-se de forma bem clara no sistema que o tratamento dos dados pessoais se encontra sujeito a restrições.

Logo, se o titular solicitar a anonimização ou o bloqueio, poderia o controlador simplesmente eliminar os dados como uma solução mais simples? A LGPD não traz a resposta a essa pergunta, e uma melhor interpretação seria pela negativa, haja vista que se estaria dando contornos restritivos aos direitos dos titulares. Mas, para isso, seria necessário que o artigo 16 ressalvasse essa situação.

A característica prolixa de disciplinar temas redundantes também ocorre nas hipóteses de excludentes de responsabilidade no artigo 43. O primeiro diz que o agente não é responsável se ele não realizar o tratamento de dados pessoais. Essa é decorrência do princípio da legalidade: ninguém poderá ser responsabilizado por ato ilícito que não cometeu, pois, se algo não é vedado por norma, não é ilícito.

O segundo inciso, que prescreve que embora tenha havido o tratamento, não houve a violação à LGPD, é decorrência lógica do princípio da responsabilização do Código Civil (artigo 186). Se não houve ato ilícito, não há responsabilidade. Conforme afirma OLIVA (2020, p. 348):

> Considera-se ato ilícito a conduta culposa ou dolosa contrária ao direito que gera dano a outrem e deflagra o dever de indenizar (CC, art. 186). O pressuposto da responsabilidade civil subjetiva é a prática do ato ilícito. Nela, valora-se a conduta do causador do dano, de maneira a aferir se obrou com culpa ou dolo, indispensáveis à noção de ilícito e,

> conseguintemente, ao dever de reparar com fundamento na responsabilidade civil subjetiva. Não releva distinguir se o autor do ilícito agiu dolosa ou culposamente, pois, em qualquer caso, a consequência é a mesma: reparação dos danos causados.

O último inciso afasta a responsabilidade em caso de culpa exclusiva da vítima ou de terceiro, o que é própria decorrência da teoria da causalidade da responsabilidade civil. Dos três incisos, talvez este último seja o mais aplicável para os fins a que se presta, até porque, como demonstra CAVALIERI FILHO (2015, p. 97), a legislação e a jurisprudência podem não admitir a culpa de terceiro como excludente da responsabilidade. Ressalva que:

> [...] No caso de bancos, por exemplo, nem mesmo o fato doloso de terceiro (assalto etc.) é admitido como excludente de responsabilidade (item 121.3). No contrato de transporte, o próprio Código Civil, em seu art. 735, não admite a exclusão da responsabilidade do transportador por fato culposo de terceiro. E a jurisprudência vem relutando em admitir a exclusão até mesmo por fato doloso (itens 93.3 e 93.4).

Não obstante, quando o inciso III se enquadrar em uma situação fática, o inciso I também poderá ser aplicável em muitas situações, visto que, se é culpa exclusiva de terceiro, o agente de tratamento pode não ter realizado o tratamento de dados pessoais.

1.3.4. O artigo 50 da LGPD

O artigo 50 da LGPD talvez seja um dos mais problemáticos em termos de legística. Sua compreensão é árdua, mesmo para especialistas no setor, e os dispositivos são repetitivos no que se refere a regulamentar o assunto. O artigo 50 trata das boas práticas e de governança que podem ser feitas individualmente ou no seio de associações, representando o que UNES PEREIRA e ALVIM (2020) denominam **autorregulação** no âmbito de privacidade e proteção de dados

pessoais. Dessa forma, o próprio agente de tratamento ou entidades que o representem poderiam elaborar suas regras e submetê-las à validação e homologação da ANPD.

O artigo 50 é redundante em alguns aspectos e de difícil interpretação, razão pela qual vale a análise apartada e sistematizada de cada um de seus requisitos para que fique mais evidente a *mens legis* do dispositivo. Segundo o *caput* do artigo em comento, essas regras deverão estabelecer:

> (i) as condições de organização;
>
> (ii) o regime de funcionamento;
>
> (iii) os procedimentos, incluindo reclamações e petições de titulares;
>
> (iv) as normas de segurança;
>
> (v) os padrões técnicos;
>
> (vi) as obrigações específicas para os diversos envolvidos no tratamento;
>
> (vii) as ações educativas;
>
> (viii) os mecanismos internos de supervisão e de mitigação de riscos; e
>
> (ix) outros aspectos relacionados ao tratamento de dados pessoais.

Podemos agrupar os requisitos do *caput* em algumas categorias: que as regras de boas práticas e de governança devem respeitar o perfil da organização [(i) e (ii)], normas de segurança da informação [(iv) e (v)] e políticas e procedimentos internos específicos [(iii), (vi), (vii) e (viii)]. Talvez tenha faltado esse tipo de categorização no *caput*.

No momento do estabelecimento dessas boas práticas, o § 1º do artigo 50 menciona que o controlador e operador,[18] no que se refere ao tratamento e aos dados, devem levar em consideração:

> (i) a natureza;
>
> (ii) o escopo;
>
> (iii) a finalidade; e
>
> (iv) a probabilidade e a gravidade dos riscos e dos benefícios decorrentes de tratamento de dados do titular.

Aqui se percebe que o enfoque desse parágrafo é a governança de dados, devendo a organização se atentar às categorias de dados [(i)], ou seja, se são pessoais, pessoais sensíveis ou de alto risco, devendo estar sempre alerta à correta definição da finalidade [(ii) e (iii)] e a avaliação de risco de privacidade em relação à probabilidade e impacto [(iv)].

Diferentemente das regras de boas práticas, as quais, no processo de autorregulação, poderiam se aplicar à empresa que pleiteia seu reconhecimento ou à entidade representativa da categoria do setor envolvido, o § 2º menciona que o controlador, para cumprir com os princípios da segurança e prevenção do artigo 6º, poderá implementar programa de governança em privacidade (inciso I) e demonstrar sua efetividade a pedido da ANPD ou outra entidade responsável por promover o cumprimento de boas práticas ou códigos de conduta. Para tanto, deve ser observado o seguinte:

> (i) a estrutura, a escala e o volume de suas operações; bem como
>
> (ii) a sensibilidade dos dados tratados; e

[18] Poderia constar no dispositivo a expressão “agentes de tratamento” em vez de “controlador e operador”.

> (iii) a probabilidade e a gravidade dos danos para os titulares dos dados.

Os requisitos anteriores resgatam a ideia de estabelecer o perfil da organização, tal como previsto no *caput*, para que as práticas sejam "customizadas" de acordo com a atividade econômica e o porte da organização que decida tratar dados pessoais.

Aqui se nota certa redundância no que se refere à observância para a estruturação do programa de governança em privacidade e ao estabelecimento de regras de boas práticas, ao exigir a análise de probabilidade e gravidade dos riscos (no segundo caso) ou dos danos (no primeiro caso). Na realidade, a própria troca da terminologia gera confusão se a intenção é disciplinar o risco ou o dano potencialmente causado (que seria a própria materialização do risco).

O programa de governança deve minimamente indicar os seguintes elementos representados nas alíneas do inciso II (que também aparecem em redundância ao já visto):

> a) demonstre o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais;
>
> b) seja aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta;[19]
>
> c) seja adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados;[20]
>
> d) estabeleça políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade;
>
> e) tenha o objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular;
>
> f) esteja integrado a sua estrutura geral de governança e estabeleça e aplique mecanismos de supervisão internos e externos;

[19] Aqui o mais correto seria abranger "operação de tratamento", e não somente a coleta – espécie do gênero "tratamento".
[20] Dispositivo redundante com o conteúdo do parágrafo segundo.

> g) conte com planos de resposta a incidentes e remediação; e
>
> h) seja atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas.

No que concerne ao conteúdo do programa de governança em privacidade, é possível extrair alguns pilares importantes: as organizações devem ter *tone at the top*, ou seja, o comprometimento da alta administração e demais colaboradores (a), a governança de dados (b), o perfil da organização (c), a análise de riscos de privacidade (d), políticas e procedimentos estabelecidos (e) e (g), uma estrutura e instância responsável (f), que será exercida pelo encarregado, e revisões periódicas do programa (h).

A doutrina indica que cada controlador ficará responsável por construir seu programa de governança de acordo com as balizas indicadas neste dispositivo – as quais, conforme observado, geram bastante confusão em relação à forma de estruturação:

> Além dos parâmetros indicados pela autoridade nacional, cada empresa privada ou órgão público poderá criar programa de governança em privacidade, segundo critérios mínimos definidos pela Lei (art. 50 da LGPD). [...] Fica estabelecido também, alcançando a Administração Pública, o dever de comunicação da ocorrência de incidentes de segurança no tratamento de dados pessoais e que possam acarretar dano potencial ou efetivo aos seus titulares (art. 48 da LGPD). (GLASSMAN, 2020, p. 875)

Na realidade, não seria necessária a regulamentação de um programa de governança por meio de dispositivo legislativo; somente sua previsão já seria adequada, e sua estrutura poderia ser regulamentada por ato infralegal. Como exemplo análogo, a Lei nº 12.846/2013, conhecida como Lei da Empresa Limpa, estabeleceu em seu artigo 7º, VIII, que a existência de um programa de integridade será levada em consideração para a aplicação das sanções.

Todavia, a lei não estabeleceu qual seria o conteúdo desse programa de integridade, cabendo à regulamentação infralegal fazê-lo. *In casu*, o Capítulo IV do

Decreto nº 8.420/2015 acabou delineando o conceito do programa de integridade e seu conteúdo mínimo nos artigos 41 e 42, respectivamente.

Por conseguinte, o mais adequado seria a ANPD elaborar cartilhas e fixar diretrizes sobre o conteúdo mínimo de boas práticas aplicáveis e também do programa de governança em privacidade, a fim de que seja possível dar melhor aplicabilidade ao prolixo artigo 50 da LGPD.

1.3.5. Fundamentos e princípios que disciplinam a proteção de dados pessoais

A LGPD é uma lei bastante principiológica e, inclusive, traz fundamentos e a definição dos seus princípios norteadores. Em vez de seguir um método de abstração por meio do modelo indutivo (ou seja, com a doutrina extraindo os princípios mediante as regras existentes), optou-se por um método de abstração por meio do modelo dedutivo (os princípios existiriam por si só, independentemente das regras que dariam o seu substrato) (DRIGO, 2013).

O artigo 2º da LGPD vislumbra que a disciplina da proteção de dados pessoais segue os seguintes fundamentos:

> Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:
>
> I – o respeito à privacidade;
>
> II – a autodeterminação informativa;
>
> III – a liberdade de expressão, de informação, de comunicação e de opinião;
>
> IV – a inviolabilidade da intimidade, da honra e da imagem;
>
> V – o desenvolvimento econômico e tecnológico e a inovação;
>
> VI – a livre iniciativa, a livre concorrência e a defesa do consumidor; e
>
> VII – os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

O inciso I é decorrência do que já foi exposto.[21] O respeito à privacidade dá-se por meio da proteção de dados pessoais, e a lei é fundamentada pelo respeito à privacidade, em um processo de retroalimentação. Dessa maneira, natural que seja um de seus primeiros fundamentos.

Já o inciso II merece maiores delineamentos. Nas palavras de SERAFINO (2020, p. 242), "a autodeterminação informativa reconhece a possibilidade de tratamento de dados, desde que seu titular tenha visibilidade sobre as atividades daqueles que os utilizam e o respaldo da legalidade em sua finalidade de tratamento".

A LGPD tenta, portanto, resgatar o titular de dados para o processo de tomada de decisões em relação ao tratamento de dados pessoais, relembrando aqueles que se imiscuírem nessa atividade de que os dados pertencem, em última instância, ao titular, e ele deve ter voz ativa no processo de tomada de decisões.

A autodeterminação informativa é um conceito-chave nesse processo, visto que recoloca o titular no centro das atenções no que se refere a seus dados pessoais. Reforça assim o conceito de que o "dono" dos dados não é a empresa que os organizou em um banco de dados, e sim a própria pessoa natural.

Nos últimos anos, tem sido comum algumas empresas entenderem erroneamente que, por criarem robustos e estruturados bancos de dados, seriam as proprietárias dessa informação em detrimento dos titulares desses dados. Consoante, destaca BARBIERI (2019, p. 18, Figura 1), existem os **dados estruturados**, como *templates* e campos, e **dados não estruturados**, como som, imagem, foto, dentre outros.

Os dados estruturados teriam maior valor para as organizações, pois poderiam ter aproveitamento econômico em larga escala para a respectiva atividade empresarial, diferentemente dos dados não estruturados, cujo aproveitamento é mais complicado em razão da falta de organização inerente ao processo de tratamento. E, em razão desse maior valor, algumas empresas poderiam fazer disso uma atividade econômica.

---

[21] Conforme capítulo 1.1.

De fato, os incisos V e VI ressaltam que a LGPD não vem para solapar a atividade econômica e a livre iniciativa, reforçando que esses também são seus fundamentos. No entanto, ao se conjugar com o inciso II, percebe-se que o desenvolvimento tecnológico e as atividades econômicas devem vir em observância ao fundamento da autodeterminação informativa.

O inciso III ressalta a questão da liberdade de expressão, informação, comunicação e opinião, o que é reforçado pelo conteúdo do artigo 4º,inciso II, alíneas “a” e “b”, subtraindo as atividades jornalísticas e artísticas do âmbito de aplicação da LGPD, e submetendo as atividades acadêmicas apenas aos artigos 7º (tratamento de dados pessoais) e 11º (tratamento de dados pessoais sensíveis) da LGPD. Ambos os dispositivos possuem incisos (IV e II, alínea “c”, respectivamente) que consubstanciam a possibilidade de tratamento de dados pessoais para a realização de estudos por órgão de pesquisa, tendo garantida, quando possível, a anonimização dos dados.

Quanto ao inciso IV, a LGPD trouxe também o fundamento do respeito à honra e à imagem, tendo como supedâneo o Código Civil. Um tema, no entanto, careceu de regulamentação: o acesso a informações pessoais de pessoas falecidas. Consoante o Considerando nº 27 do GDPR, a norma não se aplica aos falecidos. A LGPD, nesse sentido, é omissa e não detalha se há aplicabilidade ou não nesse caso. Ao conceituar dado pessoal, a LGPD define, no artigo 5º, inciso I, como sendo informação relacionada a pessoa natural. O Código Civil, no artigo 6º, por sua vez, define que a “existência da pessoa natural termina com a morte”.

Logo, surge a dúvida se a LGPD se aplicaria ou não a pessoas falecidas. Os dados dessas pessoas não seriam dados de pessoa natural, portanto, não seriam dados pessoais, e os direitos previstos na LGPD teriam de ser tutelados pelos direitos de personalidade do Capítulo II.

Nessa linha, o Decreto nº 7.724/2012, no artigo 55, parágrafo único, consigna que:

> Caso o titular das informações pessoais esteja morto ou ausente, os direitos de que trata este artigo assistem ao cônjuge ou companheiro, aos descendentes ou ascendentes, conforme o disposto no parágrafo único do art. 20 da Lei nº 10.406, de 10 de janeiro de 2002, e na Lei nº 9.278, de 10 de maio de 1996.

Logo, na linha da regulamentação da LAI, entendemos que a melhor interpretação é que caberia aos descendentes ou ascendentes o exercício dos direitos do falecido no que se refere ao tratamento de dados (independentemente de serem considerados juridicamente como dados pessoais pela LGPD), com base no artigo 20 do Código Civil e nos direitos de personalidade e tutela da honra e imagem.

Por fim, o inciso VII relaciona-se com os fundamentos basilares do país, inclusive insculpidos no artigo 1º da Constituição da República Federativa do Brasil, a saber:

> Preliminarmente, é importante destacar que esses direitos aqui tratados, decorrentes da proteção de dados pessoais, são direitos fundamentais, pois decorre do corolário da dignidade da pessoa humana previsto no art. 1º, inc. III da LGPD. Nesse sentido, há uma proposta de emenda à Constituição para estabelecer no texto constitucional esse direito dentre os direitos fundamentais previstos no art. 5º da CF/88. Outrossim, o art. 17 da LGPD estabelece a garantia de direitos fundamentais de liberdade, de intimidade e de privacidade, aos quais deve ser acrescentado o direito à proteção de dados pessoais. (LIMA; RAMIRO, 2020, p. 254)

O artigo 6º, por sua vez, é o que veicula os princípios[22] aplicáveis no âmbito das atividades de tratamento de dados pessoais, trazendo o diálogo entre as

[22] Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
I – finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
II – adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
III – necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
IV – livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
V – qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

liberdades positivas e negativas, tal como já aventado. Nesse sentido, a doutrina mais consolidada esclarece:

> Os princípios do artigo 6º da LGPD consistem em autêntico filtro de validade e legitimidade das regas de proteção de dados pessoais, que se materializa quando se verifica que a execução das políticas públicas está em equilíbrio com as liberdades positiva (controle da atividade pública) e negativa (preservação dos direitos e garantias fundamentais) do titular de dados. (TASSO, 2019, p. 275)

Conforme destacado no início do capítulo, a LGPD é bem direta e explícita ao mencionar os princípios e defini-los normativamente, sem deixar muitas brechas interpretativas para a atividade doutrinária do que seria o conteúdo mínimo de cada princípio. Nesse sentido, são dez princípios trazidos de maneira bastante conceitual.

É possível dividir esses princípios em blocos interpretativos. Os três primeiros e o penúltimo (finalidade, adequação, necessidade e não discriminação) tratam de premissas para que a operação de tratamento de dados pessoais seja lícita,[23] ou seja, o foco deontológico é definir a operação de tratamento de dados pessoais.

Se condensarmos o conteúdo desses três princípios em um feixe conceitual único, podemos concluir que o tratamento de dados pessoais é lícito quando tem uma finalidade legítima, específica, explícita e informada, correspondendo na

---

VI – transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
VII – segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
VIII – prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
IX – não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
X – responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

[23] O GDPR utiliza a expressão “licitude do tratamento” no artigo 6º para construir as bases legais em que é possível o tratamento de dados pessoais.

prática ao que é informado efetiva e previamente ao titular, reduzindo-se ao mínimo necessário em relação ao volume de dados pessoais para atingir essa finalidade, e sem possibilidade de discriminação do titular de dados em razão da operação de tratamento.

Para saber se o tratamento está adequado sob o ponto de vista da LGPD, é importante realizar um “teste de finalidade”, “teste de necessidade” e “teste de adequação”. O primeiro deles vai responder à seguinte pergunta: “Por que tratar esse dado?”. O segundo responderá à pergunta: “Quais dados você precisa minimamente para atingir essa finalidade?”. O terceiro teste vai ser uma espécie de “controle de qualidade” de todo o processo, verificando, na prática, se o tratamento está em conformidade com a finalidade apontada inicialmente.

O segundo conjunto de princípios é o do livre acesso, qualidade e transparência. Aqui, o foco deontológico dos princípios é o titular de dados pessoais, ou, em outras palavras, evidenciar que surgem novos direitos na LGPD para a pessoa natural quando do tratamento de seus dados pessoais.

Assim, o titular de dados pessoais deve poder consultar e ter informações sobre seus dados pessoais e operações de tratamento, de maneira facilitada, podendo atualizá-los e auditá-los, e exigindo informações claras e acessíveis sobre essas operações.

O terceiro conjunto é o relativo à governança em privacidade, com os princípios da segurança, prevenção e responsabilização e prestação de contas. O foco deontológico desse agrupamento são os agentes de tratamento, que precisam estruturar um programa de governança e *compliance* focado em prevenção e detecção, que traga o mínimo de medidas técnicas e administrativas aptas para proteger os dados pessoais. Essa atividade precisa ser demonstrável, ou seja, estar sempre à disposição das partes interessadas para que possam verificar sua eficácia (titulares de dados, ANPD, órgãos e entidades públicas e a sociedade em geral).

Há dúvidas se o setor público (especificamente no que se refere à administração direta) deveria estruturar um programa de governança em privacidade, sobretudo pela ausência de disposição legal. O artigo 52, § 1º, IX, coloca como uma atenuante em eventual penalidade a ser aplicada pela ANPD, e isso é bem exemplificado pela doutrina:

> Não há, portanto, como deixar de observar um conjunto bastante expressivo de regras 'gerais', aplicáveis ao tratamento de dados pessoais indistintamente da natureza jurídica do agente de tratamento.
>
> [...]
>
> Evidentemente que, sendo o caso das exceções de aplicabilidade material postas, o ente estatal poderá estar isento, entre outras, de consequências sancionatórias previstas na LGPD, mas nem por isso deve furtar-se a implementar as boas práticas que a lei sugere sejam adotadas, pois, ao final, é da proteção de direitos fundamentais que a legislação trata. (ALVES, 2020a, p. 179)

Embora não exista nenhum comando legal expresso nesse sentido, é importante que o poder público traga o exemplo que "vem de cima" (o *tone at the top*), para que as empresas possam verificar que a administração pública brasileira adere à LGPD e possui um programa interno para garantir a não violação da norma. Nesse sentido, vemos a importância desse tema no contexto de tratamento de dados pessoais no setor público, pois o mau exemplo dado pelo gestor pode contaminar todo o órgão.

Por fim, há que se considerar que a própria ANPD precisa cumprir seus misteres públicos, dentre eles atuar como agente fiscalizador do cumprimento da norma, não podendo se esquivar de sua atividade sancionatória, o que será fundamental para garantir o *enforcement* (efetividade) da LGPD. Nos dizeres de UNES PEREIRA (2020, p. 90), "[s]ancionar significa impor determinada consequência desfavorável a alguém em razão do cometimento de ilícito". Logo, em se tratando de um ilícito civil e administrativo, a ANPD precisa zelar pela responsabilização administrativa dos controladores e operadores, visto que a responsabilidade civil será tutelada por outros meios – por exemplo, judicialmente pelos próprios titulares.

Como destacado por SANTI; MAFRA (2021, p. 143), a LGPD não define expressamente o regime de responsabilização específico para a Administração Pública, trazendo o regime geral de responsabilização existente no direito público. CURY (2020, p. 141) levanta a hipótese de responsabilidade da ANPD em caso de não cumprimento de seus respectivos deveres legais, o que poderia levar à

responsabilidade subjetiva ou objetiva, dependendo do caso. Mas um ponto relevante levantado pelo autor é que a omissão da ANPD em agir pode aumentar os danos causados aos titulares de dados:

> Conclusivamente, ressalta-se apenas o cuidado necessário para não se punir os agentes públicos com as severas penas de improbidade nos casos em que a não conformidade com os ditames da LGPD seja decorrente do descumprimento disseminado da Administração Pública em relação ao seu dever legal, devendo os órgãos de controle ter uma 'sensibilidade analítica' para discernir a culpa grave ou o dolo do agente público na ausência de meios para a efetiva implementação da LGPD. (FEIGELSON; WILSON, 2020, p. 118)

Com isso, percebe-se a interferência que a LGPD possui na administração pública, sobretudo por meio da análise dos dispositivos. O próximo passo é verificar como é feito o diálogo da atividade tributária com a LGPD, o que vai trazer uma maior interface do direito público com a privacidade e proteção de dados pessoais.

2. A relação da tributação com a proteção de dados pessoais

Any tax is a discouragement and therefore a regulation so far as it goes.

Oliver Wendell Holmes Jr.

2.1. Harmonização de princípios e dos direitos das pessoas naturais e contribuintes

A seara do direito tributário é resultado da subdivisão feita pela doutrina entre direito público e privado, pertencendo à seara pública. Como o direito tributário rege a relação entre fisco e contribuinte, sendo uma das partes pertencentes à administração pública, é natural que o influxo de normas de direito público seja preponderante nessa ciência.

Em resumo, as normas incidentes sobre o direito tributário são, eminentemente, de direito público e se inspiram nos princípios gerais dessa seara, como a supremacia e a indisponibilidade do interesse público. WIMMER (2020, p. 277) destaca que:

> Tratando especificamente do tema da privacidade e da proteção de dados pessoais, diferentes autores têm discutido as dificuldades para o balanceamento entre a privacidade e outros interesses contrapostos, salientando que na raiz de tais dificuldades se encontra, de um lado, a dificuldade de quantificar um valor complexo como o da privacidade; e, de outro, a frequente caracterização de direitos associados à privacidade como sendo de natureza essencialmente individual, o que os coloca em situação desfavorável quando confrontados com o interesse público mais amplo.

As normas de proteção de dados pessoais, com exceção da LAI, costumam ser concebidas tendo em vista de maneira preponderante as relações jurídicas privatísticas, como observado no capítulo anterior. Quando se trata da proteção de dados no setor público, existe todo um regime constitucional e legal que traz poderes exorbitantes para a Administração Pública, colocando-a em posição de supremacia em relação ao particular.

Embora existam conceitos de direito público na LGPD, este não é seu foco principal, como ocorre no caso da LAI. Uma demonstração disso é a pouca disciplina trazida no que se refere ao tratamento de dados pelo setor público no

Capítulo IV da LGPD, quando, na verdade, deveria haver um regramento mais detalhado para o setor. Pode se concluir, portanto, que o tratamento de dados que envolve o setor público teve uma disciplina residual e, diante disso, com pouca ênfase aos princípios e regras gerais de direito público.

Uma opção para dar maior enfoque ao tratamento de dados pessoais do setor público seria haver uma "LGPD pública". Nesse caso, coexistiriam duas leis que disciplinariam o tratamento de dados pessoais no País: uma voltada somente para as relações privadas, e outra para as relações públicas. Embora na União Europeia não tenha sido este o caminho trilhado, conforme expõe SEER (2020) no contexto alemão, aqui isso poderia ser pertinente em virtude do tamanho da Administração Pública brasileira e seus diversos níveis federativos[24].

O regime híbrido, conforme destacado no capítulo anterior, trouxe algumas confusões conceituais que exige uma interpretação doutrinária mais acurada para se ter maiores contornos em relação à administração pública, em especial no que se refere às relações do setor público com a LGPD. WIMMER (2021, pp. 278-279), seguindo nessa linha de pensamento publicista, salienta os desafios da aplicação da LGPD no âmbito do setor público, motivo de diversos embates doutrinários:

> [...] Não faria sentido conceber que um cidadão pudesse requerer ao Poder Público a portabilidade de seus dados constantes de determinada base de dados governamentais, ou que alguém pudesse se dirigir a um cartório para solicitar a eliminação de seus dados pessoais, ou, ainda, que se pretendesse negar consentimento para que a Receita Federal processasse uma determinada declaração de imposto de renda. [...]

Essa dificuldade doutrinária, evidentemente, não afasta o regime de aplicação da LGPD na atividade tributária – em especial, na arrecadação de quaisquer tributos. Interpretação semelhante é feita no contexto alemão em relação à administração tributária e o GDPR: "[o] legislador histórico alemão e a

[24] Essa "LGPD pública" não alcançaria as relações tributárias que exigem tratamento de dados pessoais, as quais poderiam ser disciplinadas no Código Tributário Nacional. Esse ponto será mais bem desenvolvido no capítulo subsequente.

administração tributária assumem, como é óbvio, uma ampla e abrangente aplicação do RGPD a todos os tributos" (SEER, 2020, p. 31).

As administrações tributárias ocupam um lugar especial no que se refere ao tratamento de dados pessoais dentro do setor público, haja vista que a atividade tributária é, em boa parte, fundamentada no tratamento de dados pessoais. Todavia, ao se tratar das administrações tributárias, é necessário conhecer o seu conceito plurívoco, conforme explana COSTA (2017, p. 334):

> O conceito de *Administração Tributária*, em nosso entender, pode ser compreendido em dupla acepção.
>
> Em sentido *subjetivo*, primeiramente, compreende o aparelhamento burocrático mantido pelos entes autorizados a tributar, composto por múltiplos órgãos, incumbidos da arrecadação e da fiscalização de tributos.
>
> Já em sentido *objetivo*, a Administração Tributária traduz a atividade administrativa destinada a realizar a aplicação da lei fiscal, visando ao atendimento às finalidades de interesse público consubstanciadas na proteção dos direitos dos contribuintes e na arrecadação tributária. Assim, sujeita-se ao regime jurídico próprio da Administração Pública, devendo observar os princípios a ela pertinentes, especialmente os da *legalidade* e da *finalidade pública* (art. 37, *caput*, CR).

Nesse sentido, o recorte que se pretende dar neste capítulo é em relação à aplicação dos postulados de proteção de dados na atividade tributária dos diversos fiscos no Brasil. Há duas perspectivas para essa análise: uma sob o ponto de vista da atividade de exação tributária (ou seja, sob o olhar do fisco), e outra sob o ponto de vista da incidência da relação jurídico-tributária (sob a visão do titular de dados contribuinte).

A primeira – ou seja, sob a perspectiva da atividade das administrações tributárias brasileiras e as formas de tratamento de dados pessoais no âmbito interno –[25] não é o objeto de estudo deste trabalho. Por esse motivo o enfoque será

[25] Por exemplo, uma das discussões a serem travadas seria como as administrações tributárias tratam os dados de seus colaboradores. Porém não é este o enfoque do presente trabalho.

dado à perspectiva da relação jurídico-tributária, visto que é a que afeta o titular dos dados pessoais externo ao fisco, ou seja, a figura do contribuinte.

Por conseguinte, no que se refere à segunda perspectiva, o ponto de análise é o próprio tributo em si e a forma de sua exação. Na sociedade informacional, cada vez mais os dados pessoais servem para configurar a relação jurídico-tributária, em especial nas ações junto ao meio virtual (que se intensificou com a pandemia de Covid-19):

> A despeito disso, é inegável que a economia digital resulta na ausência da criação de laços físicos nos mercados consumidores; o elemento virtual é suficiente para a geração de receitas das empresas. Dito em outras palavras, é possível afirmar que os ativos imobilizados deixaram de ser relevantes à determinação do valor de uma companhia, tendo tal lugar sido ocupado pelos ativos intangíveis (GOMES *et al.*, 2018, p. 45).

Com essa maior "virtualização" da economia desde os anos 2020, é inegável que o tratamento de volumosos dados pessoais passe a ser a principal fonte de informações ao setor público para que a relação jurídico-tributária possa restar caracterizada e, portanto, para que o fisco possa impor a exação tributária ao contribuinte.

O fenômeno está bastante avançado sob a égide da relação imponível tributária. Não é à toa que no Relatório do Plano de Ação nº 1 da Organização para a Cooperação e Desenvolvimento Econômico (OCDE) no projeto BEPS (*base erosion and profit shifting*) tenha estabelecido, como resposta aos problemas tributários de ordem global, a questão da introdução de um imposto sobre fluxo de dados pela internet, chamado de *bandwidth* ou *bit tax*. FALCÃO (2018, p. 951), nessa esteira, esclarece que:

> A opção 5 propõe a imposição de um tributo unilateral sob a utilização da rede de dados de internet. Tratar-se-ia da tributação de *bits*, ou dados de internet. Tal proposta denota um tributo de difícil administração e coordenação entre os países. Além disso, a imposição deste tributo requereria maior reflexão sobre a forma de operacionalização. Esta opção não ganhou tração entre países desenvolvidos ou em desenvolvimento, e não deve ser seriamente considerada como opção

> por se tratar meramente de uma opção de curto prazo. A maior parte das ações de curto prazo são caracterizadas pela adoção de medidas unilaterais que visam remediar as falhas do sistema atual pela criação de novos tipos tributários, a fim de evitar uma consequente perda na arrecadação.

As plataformas digitais em que se inserem a economia digital, conforme destacado por BATISTA e RANGEL (2018, p. 772), estão relacionadas à geração e utilização de dados – e, como ressaltam, os dados são meios para uma atividade-fim distinta. É assim, por exemplo, que mais de 95% dos 7 bilhões de dólares de faturamento são originados por meio dos anúncios de publicidade na plataforma do Facebook, como expõem os autores. E é nessa linha que uma pessoa natural "vale" perto de duzentos dólares para o Google e para o Facebook, e quase 800 dólares para a Amazon – tudo baseado, em essência, no valor que os dados pessoais dessas respectivas pessoas exibem para essas corporações (SHAH, s/d).

Logo, esse volume sem precedentes de tratamento de dados, gerando faturamentos recordes na economia global para empresas que exploram esse tipo de atividade econômica, pode acarretar sua utilização por parte dos fiscos no mundo inteiro para fins tributários. No entanto, mesmo com esse enorme volume de dados pessoais sendo tratados para fins tributários, não se pode esquecer os direitos dos contribuintes:

> Cabe ressaltar que o sistema tributário brasileiro, se, por um lado, tem uma inequívoca preocupação com a forma, notadamente quando trata de controlar o poder de tributar (legalidade, irretroatividade, anterioridade, reserva de lei complementar etc.), por outro lado, está longe de impor um regime formalista, em especial no que tange à proteção de direitos de contribuintes (imunidades, proteção da capacidade contributiva, direito a imposto não cumulativo etc.) (BECHARA; CARVALHO, 2019, p. 102).

Portanto, deve existir um amálgama entre os princípios e direitos dos titulares de dados pessoais com os princípios e direitos dos contribuintes, vislumbrados na Constituição da República Federativa do Brasil e na legislação tributária infraconstitucional. Essa relação sempre existirá quando a atividade de

tributação envolver, de maneira substancial, a atividade de tratamento de dados pessoais para permitir a imposição de tributo.

É importante destacar que alguns tributos não costumam ter impactos substanciais em relação aos direitos relativos à proteção de dados pessoais, pois dependerá sobremaneira da hipótese de incidência de referido tributo. Nesse sentido, haverá uma influência menor dos princípios e direitos da seara de proteção de dados pessoais sobre a seara tributária.

Como exemplos, os dados pessoais que mais impactam no direito tributário são aqueles relativos à vida privada (que englobam o sigilo bancário no caso das movimentações financeiras) e as informações de renda e patrimônio da pessoa natural (que envolvem o sigilo fiscal). E o fisco, tendo acesso a esses dados, não pode realizar a divulgação a terceiros por conta das próprias regras de sigilo fiscal e bancário (SERAFINO, 2020, pp. 242-243).

Os tributos que incidem sobre a renda certamente levarão a impactos significativos nos princípios e direitos relativos à proteção de dados pessoais dos titulares de dados. É o caso do Imposto de Renda Pessoa Física (IRPF), por exemplo, em que é necessário que o titular faça a declaração de ajuste anual, incluindo diversos dados pessoais, para que o fisco possa realizar o competente lançamento do tributo por homologação.

Em um futuro próximo e com o setor público detendo essas informações *a priori*, vai ser possível que a própria apuração do IRPF seja de autolançamento com base no uso de dados pessoais de maneira massiva, o que vai exigir cuidados nos controles em relação à forma como se dá essa atividade de tratamento de dados pessoais conjugada com a própria atividade da administração tributária em cobrar o tributo do contribuinte. Deve-se, nesse contexto, recordar do princípio da autodeterminação informativa ventilado no capítulo anterior.

Na visão de SEER (2020, p. 23), a autodeterminação informativa reconhecida pelo Tribunal Constitucional Federal Alemão também abrangeria os chamados **elementos individualizáveis da tributação** (como a renda ou lucro). Nesse sentido, o doutrinador alemão entende que as informações que devem ser prestadas ao fisco também estariam abrangidas por dito preceito, pois eles podem interferir nas liberdades dos cidadãos, ainda que não tenham conteúdo informativo tão extenso. Porém o mesmo jurista ressalta que este direito não é absoluto e que

precisa ser lido no contexto da participação do indivíduo em sociedade e na coletividade. Infere, portanto, que o foco do Tribunal foi recair:

> [...] sobre a doutrina chamada limite-do-limite, a partir da qual se desenvolvem o princípio da reserva de lei, o mandamento de certeza da norma e o princípio da proporcionalidade. É claro que o contribuinte não possui qualquer direito à autodeterminação informativa fiscal. Pelo contrário, o Estado tem acesso aos dados fiscais dos cidadãos e das empresas para poder realizar a efetiva igualdade na divisão da carga tributária. (SEER, 2020, p. 24)

Assim, o autor conclui que o conjunto de decisões judiciais que vieram em relação À proteção de dados tentou trazer uma harmonia entre a proteção de dados pessoais e o que chama de "intervenção tributária". Essa harmonia, não trazida expressamente na LGPD, virá talvez da jurisprudência brasileira.

2.2. O segredo comercial e industrial e a proteção de dados pessoais

Um exemplo de desafio de harmonização[26] do direito tributário com a LGPD ocorre com o fluxo contínuo de regras de direito privado, as quais terão de ser parcialmente derrogadas pelo regime de direito público próprio da atividade tributária. Aqui convém debater a questão do segredo comercial e industrial.

A LGPD é uma lei que a todo instante ressalva a importância da preservação do segredo comercial e industrial em suas interações entre controlador e operador com o titular de dados e as autoridades (em especial a ANPD). Vale a pena analisar se essas ressalvas aplicam-se na seara tributária, mas antes convém verificar quais os pontos destacados pela LGPD em relação à função do segredo comercial e industrial.

[26] Tomamos de empréstimo a expressão utilizada por SEER (2020, p. 27) ao propor a "harmonização do direito à proteção de dados provocada pelo RGPD".

Conforme apontam CHINELLATO e MORATO (2021, p. 659), existem alguns critérios para que uma informação seja considerada segredo:

> São três as características da informação confidencial, tal como relataram Javier Fernandez e Gustavo de Freitas Morais, considerada como passível de proteção em razão de sua relevância econômica como segredo industrial ou comercial: a) que seja secreta; b) que tenham sido tomadas por medidas para mantê-las secretas; c) que tenham valor para os seus titulares.

O artigo 6º, inciso VI, ao tratar do princípio da transparência – consoante tratado –, impõe que os titulares devem ter acesso às informações sobre os tratamentos, fazendo ressalva ao segredo industrial e comercial. Da mesma maneira, ao salientar o direito ao acesso facilitado às informações por parte do titular no artigo 9º, a mesma ressalva sobre o segredo em relação à forma ou duração do tratamento surge no inciso II.

Como medida de proteção desses segredos perante a ANPD, o artigo 10, § 3º, determina a exibição do relatório de impacto à proteção de dados pessoais quando o fundamento for o legítimo interesse, ou quando for determinado pela ANPD, inclusive em relação a dados sensíveis (artigo 38), também com a ressalva do segredo. E, ao disciplinar sobre a portabilidade de dados pessoais no artigo 18, inciso V, a ANPD deverá levar em consideração o segredo comercial e industrial.

Ao emitir declaração completa sobre confirmação de existência ou acesso a dados pessoais, o agente de tratamento deverá indicar a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento, observados o segredo comercial e industrial.

Quando o tratamento tiver como base legal o consentimento do titular ou for baseado em execução de contrato, o titular pode solicitar cópia eletrônica integral de seus dados, com a observância do segredo comercial e industrial. Esse procedimento deverá ser regulamentado pela ANPD, inclusive em formato que permita a utilização dos dados subsequentemente em outras operações de tratamento.

No caso de tratamento automatizado de dados pessoais que afetam os interesses do titular, este tem o direito de solicitar informações sobre os critérios e procedimentos utilizados para a decisão automatizada, desde que observados os segredos comercial e industrial (artigo 20, §1º, da LGPD).

Na hipótese de incidente de segurança que possa trazer risco ou dano relevante aos titulares, é necessário fazer a comunicação à ANPD, descrevendo as medidas técnicas e de segurança utilizadas para a proteção dos dados, também com observância dos segredos comercial e industrial (artigo 48, § 1º, inciso III).

A ANPD tem como competência zelar pela observância dos segredos comercial e industrial, tendo em vista a proteção de dados pessoais e o sigilo das informações quando protegido por lei ou quando a quebra do sigilo violar os fundamentos do artigo 2º da LGPD (artigo 55-J, inciso II). Também deve dispor sobre as formas de publicidade das operações de tratamento de dados pessoais, observando os segredos comercial e industrial (artigo 55-J, inciso X).

Percebe-se, dessa maneira, que a LGPD se preocupou de maneira intensiva em resguardar os segredos comercial e industrial, disciplinando-o em diversas situações na LGPD onde poderiam ter um potencial de violação. No direito público, sobretudo no tributário, há que se considerar uma nuance específica em relação ao tema.

No âmbito tributário, a invocação do sigilo comercial pode ter certa limitação em razão do artigo 195 do Código Tributário Nacional, que não permite que disposições legais excluam ou limitem o direito de examinar livros, arquivos, documentos, papéis dos comerciantes industriais ou produtores, ou da obrigação destes de exibi-los. Como esses documentos podem conter dados pessoais, aplica-se à LGPD – porém, o segredo comercial ou industrial não poderia ser invocado em face do fisco, mas tão somente nas relações entre as partes privadas. Nesse sentido, MACHADO (2019, p. 253) explana que:

> Com o advento do Código Tributário Nacional ficou afastada a possibilidade de invocação das regras do Código Comercial, ou de qualquer outra lei que exclua ou limite o direito de examinar mercadorias, livros, arquivos, documentos, papéis e efeitos comerciais ou fiscais. As normas que preservam o sigilo comercial prevalecem entre os particulares, mas não contra a Fazenda Pública.

Portanto, é possível concluir que, no que se refere aos sigilos comercial e industrial, a LGPD não poderia se sobrepor ao comando do Código Tributário Nacional em relação ao dever de exibição de documentos às administrações tributárias, ainda que estes contenham dados pessoais ou dados pessoais sensíveis, invocando segredo comercial, por exemplo. Dessa maneira, deve haver a harmonização da incidência do regime jurídico de direito tributário – portanto, publicístico e calcado em leis específicas – sobre as regras de direito privado contidas na LGPD.

Como a LGPD não ressalva a questão do segredo quando esta envolver uma relação de direito público, entendemos que seria mais apropriado aplicar o comando oriundo do Código Tributário Nacional, não permitindo a oposição do segredo quando envolver a atividade de exação tributária.

2.3. O sigilo fiscal e bancário e a proteção de dados pessoais

Outro tema que merece discussão na conjugação do direito tributário com a proteção de dados é o sigilo fiscal e bancário. No caso do direito tributário, existem os conceitos de sigilo fiscal e bancário que reforçam os direitos à privacidade dos contribuintes a todo instante, e eles não surgiram somente agora, com o advento da LGPD. Entretanto, por não possuírem disposição expressa na Constituição da República Federativa do Brasil, recebem contornos doutrinários extraídos de outros dispositivos constitucionais.

No que concerne ao sigilo fiscal, SERAFINO (2020, p. 242) comenta que a Constituição da República Federativa do Brasil não veicula expressamente o direito ao sigilo fiscal, e que a doutrina tem considerado como “uma espécie do gênero sigilo resguardado no art. 5º da CF”.

Nesse sentido, o sigilo fiscal é uma regra construída a partir do Código Tributário Nacional, artigo 198, colocando apenas algumas ressalvas para a divulgação de informações fiscais do contribuinte, *in verbis*:

> 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.
>
> § 1º Excetuam-se do disposto neste artigo, além dos casos previstos no art. 199, os seguintes:
>
> I – requisição de autoridade judiciária no interesse da justiça;
>
> II – solicitações de autoridade administrativa no interesse da Administração Pública, desde que seja comprovada a instauração regular de processo administrativo, no órgão ou na entidade respectiva, com o objetivo de investigar o sujeito passivo a que se refere a informação, por prática de infração administrativa.
>
> § 2º O intercâmbio de informação sigilosa, no âmbito da Administração Pública, será realizado mediante processo regularmente instaurado, e a entrega será feita pessoalmente à autoridade solicitante, mediante recibo, que formalize a transferência e assegure a preservação do sigilo.
>
> § 3º Não é vedada a divulgação de informações relativas a:
>
> I – representações fiscais para fins penais;
>
> II – inscrições na Dívida Ativa da Fazenda Pública;
>
> III – parcelamento ou moratória.

Uma distinção importante trazida por SERAFINO (2020, p. 243) é a de que a vedação constitucional e legal (o referenciado artigo 198 do Código Tributário Nacional) é em relação à **divulgação** dos dados, e não ao **acesso** às informações no que concerne à capacidade econômica do contribuinte. Portanto, essa diferenciação é importante no que se refere ao uso compartilhado de dados pessoais, que delinearemos mais à frente.

A ideia de colocar limites ao acesso sobre informações relativas ao contribuinte, com a construção do conceito de sigilo fiscal, vai em direção ao respeito à privacidade e intimidade do contribuinte. Não obstante esse fato, há duas consequências relevantes.

A primeira é a de que os dados pessoais dos titulares não podem ser utilizados indiscriminadamente pelas autoridades tributárias, devendo cingir-se à hipótese de incidência tributária, objeto de fiscalização do fisco. Com isso, resguarda-se a privacidade e a intimidade do contribuinte, que não terá sua intimidade devassada por meio de outras ações governamentais (por exemplo, fiscalizações em outras searas que não a tributária, tais como ambiental ou trabalhista).

A segunda é a de que o acesso das autoridades aos dados pessoais deve respeitar a finalidade pela qual ele é justificado, na linha do que é reforçado pelo artigo 6º, inciso I, da LGPD: não cabe às autoridades tributárias promoverem acessos indiscriminados a dados pessoais para depois, seletivamente, escolher qual será o uso em relação a essa informação. Nesse sentido, convém destacar o excerto abaixo:

> O amplo acesso das autoridades administrativas a informações referentes aos particulares, detidas por estes ou por terceiros, é limitada pelo dever de sigilo fiscal: se a autoridade administrativa teve uma informação em razão de seu ofício, é apenas no exercício deste que a informação pode ser utilizada. (SCHOUERI, 2019, p. 917)

Há que se destacar que a Portaria nº 4.820, de 19 de novembro de 2020, editou o Manual Eletrônico do Sigilo Fiscal (e-MSF) (RECEITA FEDERAL DO BRASIL, 2020). Este importante documento infralegal serve como balizador da atuação da autoridade tributária, para que sejam respeitadas as garantias constitucionais do sigilo fiscal – consoante debatido até o presente momento. Portanto, há balizas legais e infralegais na maneira como essas informações podem ser utilizadas por terceiros fora da administração pública.

Quanto ao sigilo bancário, PAULSEN (2020, p. 359) relembra que o artigo 197 do Código Tributário Nacional determina que instituições financeiras e outras figuras descritas na norma têm o dever de prestar informações sobre bens, negócios ou atividades de terceiros, mas com a ressalva, no parágrafo único, de que os fatos em que haja obrigação legal a observar segredo profissional só podem

ser exigidos por meio de autorizações legais ou judiciais, sobrepondo-se aos deveres genéricos da norma. Adverte CARVALHO (2017, p. 565) que:

> O psicólogo, o médico, o advogado, o sacerdote e tantas outas pessoas que, em virtude de seu cargo, ofício, função, ministério, atividade ou profissão, tornam-se depositárias de confidências, muitas vezes relevantíssimas para o interesse do Fisco, não estão cometidas do dever de prestar as informações previstas no art. 197.

O conteúdo do sigilo bancário, no entanto, foi mais bem regulamentado pela Lei Complementar nº 105/2001. Cumpre sublinhar que os limites traçados pela jurisprudência desde sua promulgação estão se abrandando nos últimos anos. Como as informações de contas bancárias dos contribuintes são importantes elementos para o exercício da atividade tributária, é natural que o fisco queira ter acesso a esse tipo de informação. E com a maior pressão internacional para o combate à sonegação fiscal, evasão de divisas e lavagem de dinheiro, cada vez mais os países têm flexibilizado esse tipo de garantia, não a tornando absoluta. Um exemplo disso é a Lei nº 12.683/2012, que alterou a Lei de Lavagem de Dinheiro e ampliou o leque de atividades econômicas que devem prevenir esse tipo de ilícito e comunicar ao COAF transações consideradas suspeitas.

SCHOUERI (2019, pp. 915-917) demonstra que o sigilo bancário, no Brasil, nunca foi um direito absoluto, podendo haver cedência em caso de interesse público e outros valores. Mas quem delineava os limites do direito à privacidade do qual era decorrente era o Supremo Tribunal Federal, até a edição da Lei Complementar nº 105/2001. E, juntamente com a Lei nº 10.174/2001, o STF acabou se pronunciando pela não ofensividade ao direito do contribuinte no caso de transferência de informações pelas instituições financeiras ao fisco, pois este teria também o dever de manter as informações sob sigilo. Com isso, entende o doutrinador, o contribuinte não faria jus a um exame prévio judicial, podendo administrativamente ter sua vida privada sob exame do fisco.

É importante, todavia, fazer uma leitura do interesse público conjugada com a proteção de dados pessoais, de maneira que não apareçam como conceitos que se confrontam, mas que se complementam e se reforçam (WIMMER, 2021, p. 278).

Entendemos que é nessa linha que o sigilo fiscal e bancário se harmoniza com a LGPD.

2.4. Uso compartilhado de dados pessoais não sujeitos a sigilo fiscal pelo setor público

O uso compartilhado de dados pessoais não sujeitos a sigilo fiscal no setor público é uma regra que sempre existiu, independentemente da LGPD. Porém, a fim de garantir os direitos à privacidade e intimidade e evitar abusos por parte do Estado, SERAFINO (2020, p. 241) relembra a questão da discussão alemã da **separação informacional dos poderes.**

Logo, quando se fala em uso compartilhado, geralmente a ideia é que seja realizado "intramuros", ou seja, dentro do próprio Poder da República – até mesmo para se preservar o princípio da tripartição de poderes prescrito no artigo 2º da Constituição da República Federativa do Brasil, evitando-se interferências de um Poder sobre o outro. O uso compartilhado de dados pessoais dentro do Poder Executivo implicaria que fosse entre órgãos e entidades pertencentes a esta esfera, evitando-se o fluxo de dados pessoais entre os Poderes Executivo, Legislativo e Judiciário.

Isso não quer dizer que diversos entes federativos (como União, Estados, Distrito Federal e Municípios) do mesmo Poder (*in casu,* Executivo) não possam realizar uso compartilhado – e é justamente nesse uso compartilhado interfederativo que reside a importância para as administrações tributárias e reforça o federalismo cooperativo brasileiro.

O uso compartilhado de dados pessoais para fins tributários constitui-se em ferramenta importante para a gestão fiscal realizada pelas autoridades tributárias. No entanto, a própria normativa infraconstitucional coloca limites a essas situações, para que se preserve o sigilo fiscal dos contribuintes, como desenvolvido no

capítulo anterior.[27] Por conseguinte, o artigo 199 do Código Tributário Nacional consigna que:

> 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.

Ademais, o artigo 26 da LGPD estabelece que o uso compartilhado de dados pessoais pelo poder público tem de respeitar as **finalidades específicas de execução de políticas públicas e atribuição legal** pelos órgãos e entidades públicas. Logo, esse uso compartilhado para fins tributários não pode extrapolar aquilo definido na regra de competência do órgão.

SEER (2020, p. 26), ao trazer a discussão no direito alemão, consigna que:

> Sob essa perspectiva, os deveres do contribuinte de cooperação e de divulgar seus dados ao Fisco apenas são aceitáveis quando o cidadão-contribuinte declarante é protegido contra o uso e o repasse indevidos de seus dados.

SERAFINO (2020, p. 246), por sua vez, destaca o histórico de compartilhamento de dados na seara tributária oriundo do Decreto nº 6.022/2007, ao instituir o SPED (SPED Contábil, SPED Fiscal Digital e Nota Fiscal Eletrônica). Dessa maneira, houve a possibilidade de que os dados tivessem formato estruturado e fomentassem esse tipo de prática nas administrações tributárias. Posteriormente, a Portaria RFB nº 1.384/2016 trouxe, para órgãos e entidades da Administração Pública Federal, o regime de compartilhamento de dados não sujeitos a sigilo fiscal.

---

[27] Ver item 2.2.

Com o surgimento do e-Social,[28] começaram a emergir discussões quanto à questão do compartilhamento de informações. Um possível entendimento é que tal compartilhamento teria potencial de violação à LGPD em razão do volume de dados estruturados manipulado pela administração pública:

> Considerando que o cadastro do e-Social é bastante completo, a administração das empresas sofre a tentação de compartilhar esses mesmos dados com outros interessados, como banco, por exemplo. Acontece que os dados informados no e-Social são superiores, em quantidade e qualidade, àqueles necessários em outras relações contratuais. Com isso, pode haver divulgação indevida de dados dos funcionários e outras pessoas físicas, dados que estão sob o amparo da Lei Geral de Proteção de Dados. (FERNANDES, 2019)

Conforme destaca Doneda em entrevista (LEORATTI, 2021), há a possibilidade de questionamentos a respeito do tratamento de dados pessoais realizados por parte de órgãos fazendários, como a Receita Federal do Brasil, quando estes se mostrarem muito volumosos e desproporcionais.

Esse volume de dados estruturados de praticamente todos os cidadãos brasileiros tem, inclusive, motivado *hackers* e outras pessoas mal-intencionadas a contribuir com incidentes de vazamento de dados pessoais, como ocorreu no começo de 2021 com os dados pessoais de 220 milhões de brasileiros (EXAME, 2021). Embora ainda não se possa afirmar de onde se originou o incidente, vem crescendo a preocupação em relação ao agigantamento de dados pessoais de maneira estruturada.

No caso da Bulgária, por exemplo, SERAFINO (2020, pp. 254-255) expõe um interessante estudo de caso de um incidente ocorrido na entidade fiscal equivalente à Receita Federal do Brasil. Teria havido o vazamento de dados de seguro social, renda, nome completo, data de aniversário, endereço dos cidadãos e dados objeto de compartilhamento dentro do *Common Reporting Standards*

[28] "O outro aspecto da privacidade, no setor contábil, é que muitos dados são intercambiados com diversos operadores e controladores externos. Analise cada caso, e procure ter à mão as informações, não somente dos dados compartilhados, como dos operadores e controladores que os compartilham." (POHLMANN, 2019, p. 177)

(CRS) e da Diretiva da União Europeia sobre Cooperação Administrativa. Como consequência, ela expõe que a Bulgária foi suspensa de trocas de informação pelo Fórum Global sobre Transparência Tributária.

Dessa maneira, percebe-se que um incidente de segurança que envolva uma administração tributária pode ter consequências não somente no país, mas também em acordos de cooperação internacional do quais esses países são signatários, visto que uma suspensão fatalmente será uma medida protetiva para que não haja vazamentos ulteriores. Essa preocupação deverá ser prioridade nos fiscos nacionais.

No caso pátrio, muitas normativas recentes trouxeram novidades no que se refere ao uso compartilhado de dados pela administração pública. SERAFINO (2020, p. 249 e p. 254) destaca a edição do Decreto nº 10.046/2019, que versa sobre o Cadastro Base do Cidadão. Segundo a autora, tal cadastro utilizará os dados disponíveis na Receita Federal do Brasil e que não estejam sujeitos a sigilo fiscal, cujo acesso se dará pelo uso de *blockchain*. A autora destaca ainda o Decreto nº 10.209/2020, que trouxe as regras de compartilhamento das informações que estão sob a proteção de sigilo fiscal.

Pode-se adicionar, outrossim, a recente Portaria RFB nº 4.255, de 27 de agosto de 2020, que veio alterar a Portaria RFB nº 2.189, de 6 de junho de 2017. Nesse sentido, para nossa análise, fizemos quatro destaques:

> (i) A autorização para disponibilização de acesso ao conjunto de dados e informações relativos à Nota Fiscal Eletrônica (NF-e) por terceiros ficou revogada a partir do dia 1º de dezembro de 2020 (art. 1º, § 3º);
>
> (ii) Ficou atestada a implementação de processo de identificação de risco institucional ou risco ao sigilo individual da pessoa física ou jurídica a que se referem os dados e informações, como garantidores da conformidade com os termos do inciso I, art. 2º, da Portaria MF nº 457, de 8 de dezembro de 2016, c/c o § 2º, Art. 11, da LGPD (art. 1º, § 4º);

> (iii) O tratamento de dados pessoais constantes nas bases de dados e informações objeto da portaria ocorrem para o fiel cumprimento de políticas públicas em conformidade com inciso III, art. 7º, da LGPD (Art. 1º-A);
>
> (iv) Também houve a substituição do Anexo Único para constar a relação das categorias de dados pessoais que são objeto de disponibilização pela Serpro com o objetivo de complementação de políticas públicas (art. 1º, § 1º).

Com essas normativas mais recentes, em especial a Portaria RFB nº 4.255/2020, vêm emergindo discussões a respeito das limitações que tais normativas podem infligir a algumas atividades privadas que se utilizam de dados não sujeitos a sigilo fiscal. Alguns apontam que esse tipo de restrição pode causar problemas para negócios em que dados pessoais são imprescindíveis para o desenvolvimento da atividade da empresa.[29] Logo:

> Será absolutamente essencial que as licenças para acesso a dados por parte dos servidores públicos (que a lei a vigorar deu) tenha uma regulamentação clara e muito transparente para evitar o arbítrio e o excesso, bem assim o recrudescimento das limitações à atividade econômica que os cadastros abertos ao público causam. Do mesmo modo, há a necessidade de se prever autonomia aos órgãos de proteção de dados para aplicação de sanções ao poder público quando de infrações decorrentes de sua conduta. (PUGLIESI; GUNDIM, 2020, p. 497)

Entretanto, entendemos que, com a realidade trazida pela LGPD, muitos desses negócios, que, inclusive, realizam "raspagem"[30] de dados de acesso

[29] NOGUEIRA, 2020.

[30] Sobre a raspagem de dados: "Capturar só uma informação não basta, é preciso enriquecer esse dado. Na raspagem, a varredura consegue associar, classificar e organizar as informações coletadas. 'É um processo automatizado de busca, cópia e classificação

público, terão de se adaptar às regras e princípios estabelecidos pela nova norma. Há uma ilusão, por parte de alguns setores, que, se os dados estão disponíveis publicamente, é possível fazer o que se desejar com eles. Isso, no entanto, não é verdade:

> Dados pessoais ou sensíveis não perdem a natureza ou proteção legal pelo fato de integrarem bases de dados públicos.
>
> [...]
>
> A regra de contenção ao final do inciso IV [artigo 7º] preconiza que, ainda que acessíveis publicamente, o fundamento de validade do ato de transferência deve advir do sucesso do teste de proporcionalidade para aferição, sobretudo do atendimento ao princípio da boa-fé e da finalidade, pelo qual se conclui que, ainda que acessível publicamente, o dado pessoal não pode ser transferido a entidade privada dissociado do atendimento de finalidade pública e na persecução do interesse público. (TASSO, 2019, p. 280)

E foi nessa linha que a já mencionada Lei nº 14.129/2021, que trouxe as fundações para o Governo Digital, teve um veto em seu artigo 29, § 3º, que exibia o seguinte teor:

> § 3º É facultada aos prestadores de serviços e aos órgãos e entidades públicos que tenham por objeto a execução de serviços de tratamento de informações e o processamento de dados, em relação a dados abertos já disponibilizados ao público e devidamente catalogados de acordo com o inciso XI do § 2º deste artigo, a cobrança de valor de utilização, no caso de acesso tipicamente corporativo ou institucional, contínuo e com excessiva quantidade de usuários e de requisições simultâneas, com grande volume de dados e com processamento em larga escala.

---

de dados acessíveis na internet. O programa se passa por uma pessoa ou usuário comum, acessa um site, copia e cola o dado em algum ambiente interno', explica Hiago Kin, presidente da Associação Brasileira de Segurança Cibernética." (UOL, 2020).

As razões do veto ilustraram certa tendência do Governo Federal em frear essa comercialização massiva de dados pessoais disponíveis ao público, como se depreende da Mensagem Presidencial nº 110, de 29 de março de 2021:

> A propositura legislativa estabelece que é facultada aos prestadores de serviços e aos órgãos e entidades públicos que tenham por objeto a execução de serviços de tratamento de informações e o processamento de dados, em relação a dados abertos já disponibilizados ao público e devidamente catalogados de acordo com o inciso XI do § 2º deste artigo, a cobrança de valor de utilização, no caso de acesso tipicamente corporativo ou institucional, contínuo e com excessiva quantidade de usuários e de requisições simultâneas, com grande volume de dados e com processamento em larga escala.
>
> Entretanto, embora se reconheça a boa intenção do legislador, a propositura contraria o interesse público por dispor em termos abstratos sem maiores detalhamentos sobre a possibilidade de cobrança de valor de utilização da base, com chance de soluções [*sic*] dispares a depender do órgão ou poder que o aplicar, além de criar o risco de privar determinados segmentos do uso de base, por ausência de condições financeiras.

Há que se considerar, ademais, que, na atividade tributária, pode haver também o tratamento de dados pessoais sensíveis. SEER (2020, p. 34) exemplifica com o Imposto de Renda na Alemanha e sua relação com alguns dados pessoais sensíveis, como dados de saúde, orientação sexual (mediante o estado civil), confissão religiosa, entre outros, que podem servir para calcular a respectiva dedução de impostos.

No caso de dados pessoais sensíveis, SILVEIRA (2021) aponta a preocupação com relação a julgados que envolvam dados relativos à saúde, como em uma recente decisão do Conselho Administrativo de Recursos Fiscais (CARF), que acabou proibindo uma contribuinte de fazer a dedução de gastos com *home care* de um dependente no Imposto de Renda.

A própria LGPD determina, em seu artigo 7º, § 3º, que "[o] tratamento de dados pessoais cujo acesso é público deve considerar a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização". Isso reforça que os dados serem de **acesso** público não significam que os dados **são** públicos, pois estes continuam de titularidade da pessoa natural.

Assim destacam OLIVEIRA e COTS (2020, p. 165) que o legislador diferenciou dados de acesso público daqueles que são tornados públicos pelo titular; entretanto, deixou claro que não é porque o dado é disponibilizado publicamente que merece menos proteção em razão da falta de confidencialidade.

Nesse sentido, ressaltamos que a **classificação** do dado pessoal (se é público, interno ou confidencial) em nada altera sua **natureza** de dado pessoal ou dado pessoal sensível, pois essa é uma medida técnica e administrativa apta para reduzir os riscos à privacidade dos titulares, e não uma qualificadora do conceito de dado pessoal.

Há que se destacar também o conteúdo do artigo 26, § 1º, da LGPD, que desautoriza transferir a empresas dados pessoais de base de dados pública, a não ser em situações previamente delimitadas:

> Art. 26. O uso compartilhado de dados pessoais pelo Poder Público 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.
>
> § 1º É vedado ao Poder Público transferir a entidades privadas dados pessoais constantes de bases de dados a que tenha acesso, exceto:
>
> I – em casos de execução descentralizada de atividade pública que exija a transferência, exclusivamente para esse fim específico e determinado, observado o disposto na Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação);
>
> III – nos casos em que os dados forem acessíveis publicamente, observadas as disposições desta Lei;
>
> IV – quando houver previsão legal ou a transferência for respaldada em contratos, convênios ou instrumentos congêneres; ou
>
> V – na hipótese de a transferência dos dados objetivar exclusivamente a prevenção de fraudes e irregularidades, ou proteger e resguardar a segurança e a integridade do titular dos dados, desde que vedado o tratamento para outras finalidades.

Portanto, ainda que se permita a transferência de dados acessíveis publicamente, deve-se preservar o conjunto de direitos e princípios estabelecidos

na LGPD. Outro ponto importante é resguardar a finalidade comum de tratamento de dados pessoais, o que é bem desenvolvido no contexto da União Europeia com o GDPR:

> Pelo que expõe o Grupo de Trabalho do Artigo 29, nas hipóteses em que determinada empresa responsável pelo tratamento de dados pessoais tem a obrigação legal de compartilhar dados com a Administração Pública para fins fiscais, por exemplo, apesar de os dados serem comuns, não há, nesse caso, finalidade comum do tratamento de dados pessoais, razão pela qual a empresa e a entidade do Poder Público receptora dos dados devem ser consideradas responsáveis pelo tratamento distinto. (CHAVES, 2018, p. 121)

Por derradeiro, convém destacar que o compartilhamento de dados no setor público não é algo assente e pacífico na doutrina, havendo diversas críticas conforme apontado por WIMMER (2021, p. 283), sobretudo no sentido de que o princípio da finalidade da LGPD seria um impedimento para que o Estado pudesse trafegar dados de maneira irrestrita, como se fosse uma “unidade informacional”. Há que se considerar, portanto, que a LGPD poderá influenciar esse tipo de atuação governamental.

Depreende-se que o uso compartilhado de dados pelo poder público precisa observar o novo regime trazido pela LGPD, ainda que isso implique impactos em algumas atividades privadas que se valem substancialmente de dados pessoais em bancos de dados públicos. O que vai ajudar a delinear esses contornos será perquirir a finalidade do tratamento dos dados pessoais para fins tributários.

2.5. Deveres das administrações tributárias em relação a proteção de dados pessoais

Do que foi exposto até aqui, é possível verificar que as administrações tributárias terão de adimplir com alguns deveres de controladores a fim de a sua

atividade-fim estar em harmonia com os princípios e direitos contidos na LGPD. Mesmo com todas as regras de sigilo fiscal e bancário, o maior problema será a delimitação do tratamento de dados pessoais por parte das administrações tributárias.

Nesse sentido, alguns pontos fundamentais para a boa governança de dados por parte das autoridades tributárias é a correta definição da finalidade do tratamento dos dados pessoais quando este envolver a atividade tributária, bem como a transparência na relação com o contribuinte, incluindo eventual monitoramento fiscal que possa vir a ocorrer durante esse processo.

Far-se-á, portanto, uma análise mais detida em relação a esses pontos, a fim de verificar os mais controversos atinentes aos temas.

2.5.1. A finalidade do tratamento de dados pessoais para fins tributários

Conforme desenvolvido,[31] um dos princípios para o tratamento de dados pessoais de maneira lícita é o princípio da finalidade e seu respectivo "teste de finalidade" – o que se coaduna com a **finalidade pública** exarada anteriormente por COSTA. Quando se agrega à finalidade tributária, isso significa que há uma adstrição da finalidade à atividade de exação tributária, não podendo existir tergiversação.

Segundo DI PIETRO (2021, p. 112), o princípio da supremacia do interesse público sobre o individual serviria para evitar que a autoridade passe a utilizar os poderes da administração para fins particulares ou para qualquer outra finalidade que não a pública, ocorrendo o respectivo desvio de finalidade. A mesma lógica deve ser aplicada ao direito tributário.

SCHOUERI (2019, pp. 908-909) explica que não se justificaria que, ao fiscalizar o IPTU, a administração tributária pudesse verificar a hipótese de o contribuinte ser proprietário de veículo e cobrar os impostos incidentes sobre a propriedade automotiva, devendo haver essa harmonia na fiscalização, a qual deve

[31] Ver item 1.3.

ter uma finalidade e sua respectiva limitação: “[...] é a mesma harmonia que indicará os limites da fiscalização: quanto mais distante estiver a situação fiscalizada da competência do ente tributante, tanto menor será a justificativa para a atuação da Administração Tributária”.

Por essa razão é que a finalidade do tratamento estará intrinsecamente coligada com o fato gerador da obrigação tributária. Nesse sentido, e alinhando-se às considerações de uso compartilhado de dados pessoais entre o poder público e a iniciativa privada, TASSO (2019, p. 255) prescreve o seguinte:

> Infringe o princípio da finalidade, por exemplo, o compartilhamento de dados de consumo do programa de Nota Fiscal, idealizado como política pública de controle da arrecadação, com empresas privadas que realizarão marketing digital e perfilhamento de consumo.

Como já mencionado, a finalidade de tratamento de dados pessoais para fins tributários não pode ser tergiversada, seja para a arrecadação de outros tributos que não aquele dentro da regra de competência da autoridade, seja para atividades privadas que não guardem relação com a atividade de administração tributária.

SEER (2020, p. 25) demonstra que o Tribunal Constitucional Alemão costuma ver ameaças às liberdades quando os dados podem ser utilizados de maneira cruzada ou com outras finalidades. Por conseguinte, o legislador teria que definir legalmente a **finalidade da coleta** para fins tributários, além de discriminar qual autoridade e para qual atividade se autoriza referido ato.

Um exemplo dado por SEER (2020, p. 32) é ilustrado mencionando a carta de introdução ao GDPR do Ministério da Fazenda, exibindo o seguinte trecho:

> **Exemplo**: a finalidade de tratamento dos dados pessoais coletados no âmbito da declaração de imposto de renda de 2017 consiste na apuração e cobrança do imposto de renda de 2017 (inclusive possíveis investigações dos fundamentos da tributação por meio de auditorias ou de requisição de informações a terceiros, bem como a execução, a responsabilização de terceiros ou o processo administrativo de impugnação).

Nesse diapasão, conclui o jurista que a administração tributária na Alemanha prefere trabalhar com uma concepção mais restrita no que se refere à finalidade do tratamento, adequando-se a: espécie tributária, momento da tributação e sujeito passivo. Logo, diante desse exemplo, ilustra que se os dados pessoais usados para o imposto sobre a renda fossem utilizados para lançar imposto sobre vendas no mesmo período, isso seria considerado um tratamento posterior. Para tanto, o autor, baseado no sistema tributário alemão, descreve as seis hipóteses em que esse tipo de tratamento posterior poderia ocorrer.[32]

Logo, o tratamento posterior poderia subsistir quando: ocorrer em um processo administrativo-fiscal, processo de fiscalização, processo judicial tributário, havendo relação entre o tratamento posterior e o novo processo e obedecendo o princípio da proporcionalidade (SEER, 2020, pp. 32-33).

Uma ferramenta importante para a administração pública será realizar os testes de finalidade, necessidade e adequação já argumentados, pois isso conceberá uma importante baliza para saber se o tratamento de dados pessoais pelas administrações tributárias está ou não em conformidade com a LGPD.

É oportuno repisar que o princípio da finalidade ganha outros contornos quando envolve uma relação de direito público, diferente de relações eminentemente privadas. Nesse caso, há que se respeitar o interesse público que é o legitimador da operação de tratamento de dados pessoais, trazendo um caráter dúplice ao princípio da finalidade insculpido na LGPD: além da adstrição ao conteúdo do artigo 6º, I, da norma, deve-se levar em consideração a própria finalidade pública que é inerente aos atos administrativos praticados pelas autoridades tributárias.

---

[32] SEER, 2020, pp. 32-33. “A administração tributária defende com isso uma noção mais restrita de finalidade de tratamento, que se ajusta ao tipo de espécie tributária, ao período ou momento da tributação e ao respectivo sujeito passivo (TIPKE et. al., 2018a, § 29c AO, par. 8). Assim, por exemplo, se os dados fiscais pessoais obtidos pelo mesmo agente público por meio da declaração de imposto de renda forem usados para o lançamento do imposto sobre vendas referente ao mesmo período de apuração (2017), haverá se configurado um tratamento posterior (ALEMANHA, 2018a, par. 26). Para que os dados coletados originariamente para aquela primeira finalidade possam ser usados na segunda apuração ou em outras, o § 29c, par. 1, período 1, da AO amplia o espectro de possibilidades de tratamento e elenca para tanto *seis hipóteses*”.

Além disso, não se pode olvidar que existem as questões de competências na administração pública, o que pode ensejar a invalidação caso a atividade de tratamento seja praticada por agente fora de sua competência prevista legalmente. Inclusive, a Lei de Ação Popular (Lei nº 4.717/1965) prescreve, no artigo 2º, que são nulos os atos administrativos praticados com vício de competência. No parágrafo único, alínea "a", destaca-se que "a incompetência fica caracterizada quando o ato não se incluir nas atribuições legais do agente que o praticou".

Dessarte, TASSO (2019, p. 276) sistematiza:

> Os princípios da finalidade (artigo 6º, I, da LGPD), da adequação (inciso II) e da responsabilização e prestação de contas (inciso X) buscam fundamento de validade nos princípios constitucionais da legalidade, da impessoalidade e da moralidade (artigo 37, **caput**, da Constituição Federal) e se materializam quando, cumulativamente, o ato administrativo de tratamento ou compartilhamento de dados pessoais:
>
> a) está previsto em leis e regulamentos ou respaldado em contratos, convênios ou instrumentos congêneres (artigo 7º, inciso III, da LGPD);
> b) é praticado no exercício de suas competências ou atribuições (artigo 23, **caput**, da LGPD);
> c) o ato praticado busca o atendimento do interesse público (artigo 23, **caput**, da LGPD).

Na Alemanha, SEER (2020, p. 28) destaca que a hipótese de tratamento de dados para fins tributários baseada no interesse público é insuficiente, sendo necessário um **fundamento legal especial:**

> Para o processo tributário são importantes as hipóteses de permissão do art. 6º, par. 1, alínea "e", do RGPD. De acordo com ele, o tratamento de dados é lícito na medida em que ele for necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento. Todavia, para o tratamento de dados pessoais com finalidade fiscal, os estados-membros necessitam de um fundamento legal especial, cujas hipóteses são especificadas claramente pelo art. 6º, par. 2-4, do RGPD.

A mesma problemática pode ser vista no caso do Poder Judiciário brasileiro. BAIÃO e TEIVE (2020, p. 315) descrevem que a base legal adequada para tratamento de dados pessoais nos processos judiciais não estaria dentro do artigo 7º, e sim no *caput* do art. 23. Assim, reforça-se que os fundamentos legais para o tratamento de dados pessoais pelo setor público não estão especificados nos artigos 7º e 11º, mas no capítulo destinado ao tratamento de dados pessoais pelo setor público. Porém pouco se detalha a respeito do tratamento de dados no âmbito da atividade-fim do Poder Judiciário.

Esse alinhamento da atividade de administração tributária (em especial na sua faceta de investigação) com o interesse público é fundamental, agregando-se também o respeito à proteção de dados pessoais do titular. Logo:

> Importante, outrossim, é a colocação de que a fiscalização se faz com respeito aos direitos individuais. Ou seja: não é facultado à Administração, posto que em nome do 'interesse público' de arrecadar, deixar de lado os direitos individuais. (SCHOUERI, 2019, p. 909)

No ordenamento jurídico especial trazido pela LGPD, a proteção de dados pessoais insere um novo vetor para a contenção das atividades fiscalizatórias do Estado: além das questões imperativas de direito público, como os direitos do contribuinte e o interesse público, há que se observar, igualmente, considerações de natureza de proteção de dados. Essa é a grande novidade introduzida pela LGPD.

Por exemplo, poderia a administração tributária, na atividade de fiscalização, utilizar-se de metadados para outras questões que não a atividade tributária? Segundo BARBIERI (2019, p. 15 e p. 217), o metadado é o dado sobre o dado, ou seja, traz o contexto da informação. Logo, o uso de metadados para uma atividade de exação tributária respeitaria o princípio da finalidade do tratamento de dados pessoais? Um exemplo seria o fisco analisar os metadados da emissão de uma nota fiscal eletrônica para verificar, por meio do endereço de IP, se ela está de acordo com as informações relativas à sede do contribuinte, evitando assim evasão fiscal.

Entendemos que, caso o contexto da informação seja importante – por exemplo, se realmente foi o contribuinte o responsável pelo preenchimento de uma declaração para apuração de tributo e essa informação for relevante para alguma questão fática –, esta poderia ser uma informação dentro do princípio da finalidade do tratamento de dados pessoais. É importante, contudo, que, em homenagem à transparência, o titular de dados pessoais tenha ciência de que os metadados também são elementos que podem ser utilizados em uma atividade de fiscalização e autuação.

Há que se considerar que o espírito da LGPD é de que exista a limitação ao tratamento de dados pessoais quando este desrespeitar os princípios dos titulares de dados pessoais, bem como estiverem em desacordo com os fundamentos da própria norma. Nesse sentido, na União Europeia, a sistemática é a mesma do GDPR:

> É preciso, como em geral no tratamento de dados, observar o *princípio da proporcionalidade*. Entre os princípios estabelecidos no art. 5º da RGPD para o tratamento de dados pessoais, há o princípio da minimização dos dados e da limitação de conservação (Art. 5º, par. 1, alínea “c”). No entanto, isso não equivale a uma restrita reserva de necessidade para a coleta de dados. Na verdade, o auditor fiscal competente para o primeiro tratamento dos dados goza de certo *espaço de prognose* ao decidir sobre o tratamento posterior de dados (ALEMANHA, 2017a, p. 79). Tal espaço alcança, sobretudo e fundamentalmente, a troca de informações e a assistência mútua entre os órgãos fiscais (§ 194, par. 3, AO) (ALEMANHA, 2017a, 79) (SEER, 2020, p. 33).

No que é atinente a esse espaço de prognose trazido pela doutrina alemã, pode-se traçar um paralelo com a discricionariedade administrativa à qual as administrações tributárias brasileiras gozam a fim de poder exercer sua atividade tributária. Contudo, no sistema brasileiro, há limitações à discricionariedade administrativa, definida nos contornos da lei.

Conforme ensina UNES PEREIRA (2020, pp. 102-104), a discricionariedade administrativa da teoria de Celso Antônio Bandeira de Mello veicula uma margem de liberdade para a atuação do administrador público, ou seja, ele pode tomar decisões dentro de diversas soluções possíveis. Com isso, exige-

se um processo de interpretação da norma jurídica, e não propriamente uma escolha aleatória.

Uma outra vertente é no que se refere à aplicação dos conceitos jurídicos indeterminados – ganhando maior complexidade no Direito Administrativo, visto que a aplicação do conceito não ocorre por parte interpretativa do Poder Judiciário, e sim pelo próprio administrador quando de sua atuação. A doutrina vem rechaçando a sua aplicação nessa seara, sendo o conceito de discricionariedade diferente do conceito jurídico indeterminado.

Importante destacar que a LGPD veio para trazer novos contornos à discricionariedade administrativa, além do que já dispõe a legislação tributária. Portanto, é importante que esse espaço de prognose esteja dentro dos contornos trazidos pela norma.

Em conclusão, a questão da finalidade do tratamento de dados pessoais para fins tributários no Brasil sempre será dotada de polêmica, haja vista que os contornos para fins tributários não foram muito bem delineados pela LGPD tampouco no Código Tributário Nacional, sobrando espaço regulamentar infralegal às próprias autoridades tributárias.

2.5.2. Transparência e o direito de informação do titular

O direito de informação em relação à atuação do Estado extravasa o conteúdo da proteção de dados e serve como garantia das liberdades individuais dos cidadãos. Um Estado transparente tende a ser menos arbitrário, mais sujeito ao império da lei e ao escrutínio popular, portanto, tem maior qualidade democrática.

Muitos dos princípios que regem o direito de informação em geral dos cidadãos podem ser transportados para a esfera da proteção de dados pessoais, à exemplo do **princípio da viseira aberta** no direito alemão:

> De acordo com o art. 13, par. 3, do RGPD, o responsável, isto é, a autoridade fiscal, tem a obrigação de informar ao titular sobre a finalidade da coleta de dados, o fundamento legal para o seu tratamento, os contatos do encarregado pela proteção de dados e, eventualmente, a intenção de transmitir os dados para um país terceiro (MYßEN, 2017, p. 1868). O art. 13, par. 2 exige, também, que seja informado o prazo de conservação e seja fornecido um esclarecimento acerca dos direitos do titular dos dados. O mesmo vale, nos termos do art. 13, par. 3, para os casos em que o responsável queira tratar os dados posteriormente para outras finalidades. De maneira geral, o RGPD é marcado pela ideia de *transparência* e da *proporcionalidade* (confira também os requisitos do art. 12 da RGPD). Vige o princípio da viseira aberta [*Grundsatz des offenen Visier*]. (SEER, 2020, p. 29)

Nas notas do tradutor, é explicado que o princípio da viseira aberta exige que a atuação policial seja transparente e o agente reconhecível na abordagem. No que se refere à proteção de dados pessoais, o paralelo seria o titular sempre saber quem realiza a coleta de seus dados pessoais, bem como a finalidade desse ato (SEER, 2020, p. 29, nt. 14). Nesse sentido, além de a autodeterminação informativa ser um fundamento e a transparência um princípio na LGPD, consoante já desenvolvido,[33] o artigo 9º[34] veicula o direito de acesso facilitado às informações sobre o tratamento de dados pessoais.

A LGPD reforça recorrentemente a importância de o titular de dados pessoais ser informado a todo instante das decisões em relação ao tratamento desses dados pelos controladores. Esse postulado é corolário do próprio direito à informação insculpido constitucionalmente, que possui natureza **bifronte,** conforme expõe a doutrina:

---

[33] Ver item 1.1.

[34] Art. 9º O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso:
I – finalidade específica do tratamento;
II – forma e duração do tratamento, observados os segredos comercial e industrial;
III – identificação do controlador;
IV – informações de contato do controlador;
V – informações acerca do uso compartilhado de dados pelo controlador e a finalidade;
VI – responsabilidades dos agentes que realizarão o tratamento; e
VII – direitos do titular, com menção explícita aos direitos contidos no art. 18 desta Lei.

> Considera-se, assim, o direito à informação um direito bifronte, uma vez que se manifesta, no nível do emissor, pela liberdade de expressão, isto é, pelo direito de exprimir ideias e opiniões, e, no nível do receptor, pelo direito de receber informações. (RIBEIRO, 2020, p. 303)

A transparência talvez seja um dos princípios mais importantes disciplinados na LGPD, e não é por outra razão que o acesso a informações é tema frequente na norma. Embora o mote seja a privacidade, a LGPD tem como baliza que é possível alcançá-la por meio do esclarecimento ao titular e pela informação de como os dados pessoais são utilizados pelos agentes de tratamento. Consigna DONEDA (2019, p. 325) que:

> Revela-se, então, um dos aparentes paradoxos com os quais nos deparamos: em um marco jurídico estruturado a partir da privacidade, torna-se necessário levar em conta – e mesmo promover, em diversas instâncias – a transparência. É sintomático que, no atual clima que envolve algumas discussões sobre a matéria, seja mais provável ouvir propostas do gênero de **windows are better than walls to protect our privacy** do que afirmações clássicas como a de que **la vie privée doi être murée.**

É importante que o dispositivo do artigo 9º seja concebido em aliança com o artigo 23, inciso I, da LGPD, que versa sobre o tratamento de dados no setor público, conforme a seguir:

> 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.

Depreende-se, portanto, que esses dois dispositivos da LGPD são o núcleo do cumprimento do direito de acesso às informações do titular de dados, materializado inclusive no artigo 18, incisos I e II, ao permitir o direito de confirmação da existência de tratamento e o de acesso aos dados – *in casu*, por meio de requisição direta do titular.

Dessa maneira, imprime-se (ou devolve-se) ao titular de dados o controle sobre seus dados pessoais, em homenagem à autodeterminação informativa. Embora o direito tributário possa derrogar parcialmente algumas das regras da LGPD (considerando que se trata de ramo de direito público, atendendo portanto os interesses da coletividade com a arrecadação), é preciso considerar que tal atividade derrogatória não é absoluta, e as normas e a jurisprudência desta seara vêm, há séculos, estabelecendo limites ao poder de tributar e arrecadar.

Por essa razão é que se impõe que o titular possa, dentro dos contornos da lei, ter controle sobre os seus dados usados para fins tributários:

> O principal vetor para alcançar tal objetivo é franquear ao cidadão **controle** sobre seus dados pessoais. Essa estratégia vai além do consentimento do titular dos dados, pelo qual ele autorizaria o seu uso. Tão importante quanto esse elemento volitivo é assegurar que o fluxo informacional atenda às suas legítimas expectativas e, sobretudo, não seja corrosivo ao livre desenvolvimento da sua personalidade.
>
> É a combinatória desses elementos de que se trata a autodeterminação informacional. [...] (BIONI, 2021, p. 104-105)

Ao analisar os indigitados dispositivos, é importante remeter à lição de TASSO (2019, p. 276), que sintetiza, de maneira escorreita, os principais dispositivos que se conjugam com a transparência e a publicidade (de estatura constitucional) no que se refere ao tratamento de dados pessoais:

> Os princípios da transparência (artigo 6º, inciso VI, da LGPD) e do livre acesso (inciso IV da LGPD) possuem direta relação com o princípio da publicidade (artigo 37, **caput**, da Constituição Federal) e são observados quando o órgão ou ente administrativo:

> a) pratica a transparência ativa (artigo 23, inciso I, da LGPD e artigo 8º da LAI);
> b) viabiliza a transparência passiva (artigo 23, inciso I, da LGPD e artigo 10 da LAI);
> c) implementa outras formas de publicidade das operações de tratamento preconizadas pela ANPD (artigo 23, § 1º, da LGPD);
> d) expede os informes (artigo 26, § 2º, da LGPD) e comunicados (artigo 27, inciso II, da LGPD) na forma da lei.

O artigo 23, inciso I, não consigna expressamente a forma de direito de informação ativa (ainda que pratique uma transparência ativa); todavia, existem ferramentas jurídicas no artigo 18 que permitem que o titular possa exercer seu direito de informação em relação ao tratamento dos dados pessoais, valendo para os setores privado e público. Ou seja, na inércia do Estado, o titular de dados pessoais não fica desguarnecido no que se refere às informações sobre a utilização de seus dados pessoais.

No caso da construção jurisprudencial alemã, é interessante notar que o Tribunal Constitucional daquele país entendeu que deveria ter um dispositivo específico para a esfera tributária:

> No que concerne à coleta de dados, para a qual não há obrigação do órgão administrativo de ativamente comunicar o respectivo titular acerca dela, o BVerfG considera a previsão de um *direito de informação do titular dos dados* como um elemento crucial de uma ordem jurídica que satisfaz os respectivos direitos fundamentais (ALEMANHA, 2008, p. 364). Por conseguinte, o tribunal entende ser dever do legislador criar um direito de informação semelhante dentro do processo de tributação. (SEER, 2020, p. 25)

SEER (2020, p. 27 e p. 34) destacou que a jurisprudência alemã tem reconhecido o dever de informar os titulares de dados a respeito da administração pública – em especial no que se refere ao fisco. E, no que se refere ao armazenamento, após o decurso do prazo de conservação os dados devem ser eliminados para evitar abusos. Com isso, homenageia-se a transparência em relação ao tratamento de dados, seja em coleta direta ou mediante informações de terceiros.

SEER (2020, p. 35) destaca, no entanto, que há certos limites no dever de informar, reconhecido pelo próprio GDPR. Nesse caso, haveria abstenção de informação no caso de prevenção, investigação, detecção ou repressão de infrações penais e no caso de pôr em risco as tarefas de competência da própria autoridade tributária. Nesse caso, o titular poderia ocultar ou destruir provas relacionadas aos fatos jurídicos-tributários, ou até mesmo adaptar como cumprir as obrigações tributárias para impedir a ciência do fisco em relação aos fatos geradores. É o que ocorre com o artigo 11, inciso II, da Lei nº 9.613/1998, de acordo com o qual as pessoas sujeitas aos mecanismos de prevenção à lavagem de dinheiro devem se abster de informar à pessoa suspeita de lavagem, ou a terceiros, de que foi feita uma comunicação de operação suspeita ao COAF.

Logo, impende afirmar que o dever de informar das administrações tributárias encontra derrogações específicas. Ademais, existe um importante limitador temporal à manutenção dos dados pessoais para fins tributários, que é a figura jurídica da prescrição. Nessa linha, "[e]ntre eles estão os dados referentes a períodos de apuração que já prescreveram. Se a pretensão tributária não mais existe, falta uma justificativa para se continuar mantendo os dados". (SEER, 2020, p. 38)

Uma medida importante para adoção das administrações tributárias é a elaboração de uma tabela de temporalidade que torne possível o acompanhamento dos fatos geradores sujeitos a prescrição, de modo a promover a eliminação ou anonimização desses dados pessoais caso sejam desnecessários, na linha do que dispõe o artigo 18, inciso IV, da LGPD. Logo, à linha do racional adotado pelo GDPR, os dados para fins tributários não devem ser mantidos por tempo indeterminado:

> No tocante ao aspecto temporal, o Considerando n. 9 do RGPD exige, para fins de limitar a conservação dos dados, que sejam estipulados prazos para apagamento deles. A respeito dos dados diretamente transmitidos pelo sujeito passivo pode se procurar em vão um fundamento na AO. O legislador parece partir do pressuposto de que no âmbito tributário os dados digitais estão disponíveis por tempo indeterminado. Mas isso seria contrário ao princípio da proporcionalidade no tocante à proteção jurídica de dados e ao dele decorrente princípio da minimização dos dados. (SEER, 2020, p. 39)

Também é importante que seja dada transparência a essa tabela de temporalidade para toda a população de contribuintes, para que ela tome ciência do período e da finalidade do armazenamento dos seus dados, inclusive para que possa tanto exercer o controle sobre esse processo junto às administrações tributárias, como seu contraditório e ampla defesa em caso de autuações indevidas e execuções fiscais.

Em continuação, cumpre, outrossim, analisar o veto ao artigo 28 da LGPD, que prescrevia que "a comunicação ou o uso compartilhado de dados pessoais entre órgãos e entidades de direito público será objeto de publicidade, nos termos do inciso I do caput do art. 23 desta Lei". Aparentemente, o veto não vai ao encontro dos postulados em relação à transparência aqui tratados. Nesse sentido, convém destacar o comentário de LOPES (2019, p. 140), que sintetiza os respectivos motivadores da decisão presidencial:

> Adicionalmente, insta recordar que o projeto legislativo que deu origem à LGPD abarcava, ainda, a necessidade de proteção e preservação dos dados pessoais dos requerentes de acesso à informação ao Poder Público, vedando o compartilhamento tanto no âmbito da Administração Pública quanto com pessoas jurídicas de direito privado. Ocorre que tal inciso foi vetado, por sugestão do Ministério da Fazenda, que destacou que o compartilhamento de informações é medida recorrente e essencial para o regular exercício de diversas atividades e políticas públicas. Exemplificativamente, como fundamento, foram destacados os bancos de dados da Previdência Social, do Cadastro Nacional de Informações Sociais e as investigações realizadas no âmbito do Sistema Financeiro Nacional.

Todavia, esse dispositivo merece algumas críticas, pois o motivo trazido pelo veto no sentido de que a publicidade tal como preconizada "[...] pode tornar inviável o exercício regular de algumas ações públicas como as de fiscalização,

controle e polícia administrativa"[35] não parece encontrar guarida com esse racional desenvolvido. Eis que:

> Na mesma linha, critica-se o veto dado ao art. 28 da LGPD, que determinava que se conferisse publicidade à comunicação ou ao uso compartilhado de dados pessoais entre órgãos e entidades de direito público. A razão do veto, no sentido de que o dispositivo poderia **tornar inviável o exercício regular de algumas ações públicas como as de fiscalização, controle e polícia administrativa,** também enfrenta dificuldade para se sustentar no contexto de um Estado Democrático de Direito, que tem a publicidade como princípio da Administração Pública (art. 37, **caput**, CF).
>
> É inequívoco que, com o acelerado desenvolvimento tecnológico que se observa na atualidade, há cada vez mais dispositivos que se propagam pelo espaço urbano, capazes de coletar dados sobre as pessoas, monitorar e vigiar suas atividades e até mesmo manipular seus comportamentos. (XAVIER; XAVIER; SPALER, 2020, p. 492)

Essa advertência parece caminhar justamente na linha de aumentar o monitoramento para fins fiscais, ponto que desenvolveremos no subcapítulo subsequente. Cumpre destacar, no entanto, que o argumento trazido à tona não foi ilustrado no momento do veto, ou seja, de que maneira a publicidade no compartilhamento de informações poderia prejudicar as atividades estatais ali listadas. Desse modo, convém também salientar a opinião de WIMMER (2021, pp. 275-276):

> A aparente tensão entre publicidade e privacidade tem sido ocasionalmente suscitada no contexto da necessidade de conciliar regras que impõem ao Estado um elevado grau de transparência quanto às suas atividades e aquelas que exigem que dados pessoais de cidadãos sejam tratados de maneira a preservar a sua intimidade, vida privada, honra e imagem. Normas voltadas a ampliar a transparência do Estado – como a Lei de Acesso à Informação ("LAI") e as políticas de dados abertos – muitas vezes são construídas a partir de uma lógica de classificação das

[35] Convém aqui destacar o conceito de UNES PEREIRA (2020, p. 77) para o poder de polícia: "O conceito de poder de polícia revela a principal tensão do Direito Administrativo, qual seja, o conflito entre as prerrogativas públicas e as liberdades individuais. 'Bem comum', 'interesse coletivo' ou 'interesse público' de um lado e de outro as liberdades individuais e o interesse privado."

> informações com base em seu grau de sigilo, que não necessariamente se alinha à lógica esposada por normas que tenham por objetivo a proteção de dados pessoais, como a LGPD. [...]

Uma das figuras que pode ajudar a materializar esse acesso às informações mais detalhadas acerca do tratamento de dados pessoais é o Encarregado de Proteção de Dados, figura criada pela LGPD no artigo 5º, inciso VII, como a pessoa que funciona como um "canal de comunicação" tripartite entre controlador, titulares de dados e ANPD.

Para o setor público, a LGPD estabelece a obrigatoriedade de indicação do Encarregado quando realizarem tratamento de dados pessoais, nos termos do artigo 39 da LGPD. O dispositivo disciplina como o operador deverá fazer o tratamento de dados pessoais, sempre seguindo as instruções do controlador. O artigo 41, por sua vez, em seu *caput* exige que o controlador indique um Encarregado. Portanto, no caso do setor público, a indicação do Encarregado é uma realidade que não pode ser excepcionalizada:

> [...] Sendo a categoria de pessoa jurídica prevista no caput do artigo 23, ou, ainda, se empresa pública ou sociedade de economia mista quando no exercício de políticas públicas (artigo 24), a indicação de encarregado de proteção de dados é imposição inafastável, sequer sujeita à dispensa, nos termos do artigo 41, § 3º. (ALVES, 2020b, p. 192)

Nessa linha, convém destacar a opinião de ALVES (2020b, pp. 528-529):

> Parece evidente, nesse caso, que a indicação do DPO público seja compulsória e inafastável, uma vez que se trata de *conditio sine qua non* para o tratamento de dados pessoais pelo poder público. [...]
>
> [...]
>
> Logo, somos da opinião de que os **órgãos e entes públicos que realizem tratamento de dados pessoais deverão indicar um encarregado, seja na condição de controladores, seja como operadores.** [grifos do original]

No âmbito federal, a Instrução Normativa SGD/ME nº 117, de 19 de novembro de 2020, dispôs sobre a indicação do Encarregado no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional. Portanto, no âmbito federal, a autoridade tributária poderá se valer da regulamentação existente para a indicação do referido profissional, que "deverá possuir conhecimentos multidisciplinares essenciais à sua atribuição, preferencialmente, os relativos aos temas de: privacidade e proteção de dados pessoais, análise jurídica, gestão de riscos, governança de dados e acesso à informação no setor público" (artigo 1º, § 1º, inciso I).

É possível que a autoridade tributária, em determinadas situações, não possa fornecer as informações por conta de questões relativas a sigilo fiscal ou outras limitações legais. Essa análise jurídica poderia ser realizada pelo Encarregado, por exemplo, filtrando o que poderia ser informado no caso concreto.

Nesse sentido, convém observar o precedente alemão que disciplina duas hipóteses. A primeira pode ocorrer em eventual emissão de certidão negativa de tratamento de dados pessoais:

> Se este não for o caso, a autoridade tributária deve, ao responder o pedido de informações, expedir uma certidão negativa de tratamento de dados (solicitação com resultado negativo) (TIPKE et al., 2018a, § 32c AO, par. 7). Se os dados estão sendo ou foram tratados, possui o titular uma pretensão jurídica vinculante de ser comunicado acerca da finalidade do tratamento, da categoria dos dados pessoais tratados (no caso de dados obtidos junto a terceiros, também a origem dos dados), o receptor dos dados e o prazo de conservação planejado para os mesmos. (SEER, 2020, p. 37)

A segunda é justamente quando da necessidade de negativa de informações, que deve estar bem fundamentada a fim de permitir o exercício do direito ao contraditório e devido processo legal ao contribuinte, com a possibilidade de recorrer da decisão:

> Caso o órgão fiscal negue acesso às informações com base em um requerimento do contribuinte sobre seus dados pessoais, como, por

> exemplo, uma solicitação sobre seus dados pessoais arquivados junto ao órgão fiscal, tem o contribuinte o direito de recorrer contra essa decisão ao BfDI (SEER, 2020, p. 41).

Assim, nota-se que da interação dos contribuintes com o Encarregado poderão surgir diversas questões processuais administrativas e que as administrações tributárias deverão estar preparadas, em especial aquele que for nomeado para a função.

Cumpre salientar, na esteira de ALVES (2020b, pp. 529-530), que o regime do Encarregado para as autoridades é mais claro no GDPR, como se depreende do artigo 37º e da Considerando nº 97[36]. Para o exercício da função, ALVES (2020b, p. 534 e p. 539) destaca que o Encarregado deve possuir estabilidade para o exercício da função, ou seja, não deve ser passível de exoneração *ad nutum*, na esteira do que é definido no artigo 38º, item 3, do GDPR, e no Grupo de Trabalho 29 (GT29). Essas normativas ressaltam a importância da não interferência ou retaliação ao Encarregado em razão do exercício de suas funções. Outra questão ressaltada pelo autor é que o GDPR e o GT29 também destacam a possibilidade

[36] "(97) Sempre que o tratamento dos dados for efetuado por uma autoridade pública, com exceção dos tribunais ou de autoridades judiciais independentes no exercício da sua função jurisdicional, sempre que, no setor privado, for efetuado por um responsável pelo tratamento cujas atividades principais consistam em operações de tratamento que exijam o controlo regular e sistemático do titular dos dados em grande escala, ou sempre que as atividades principais do responsável pelo tratamento ou do subcontratante consistam em operações de tratamento em grande escala de categorias especiais de dados pessoais e de dados relacionados com condenações penais e infrações, o responsável pelo tratamento destes ou o subcontratante pode ser assistido por um especialista em legislação e prática de proteção dados no controlo do cumprimento do presente regulamento a nível interno. No setor privado, as atividades principais do responsável pelo tratamento dizem respeito às suas atividades primárias e não estão relacionadas com o tratamento de dados pessoais como atividade auxiliar. O nível necessário de conhecimentos especializados deverá ser determinado, em particular, em função do tratamento de dados realizado e da proteção exigida para os dados pessoais tratados pelo responsável pelo seu tratamento ou pelo subcontratante. Estes encarregados da proteção de dados, sejam ou não empregados do responsável pelo tratamento, deverão estar em condições de desempenhar as suas funções e atribuições com independência."

"Artigo 37º
Designação do encarregado da proteção de dados
1. O responsável pelo tratamento e o subcontratante designam um encarregado da proteção de dados sempre que:
a) O tratamento for efetuado por uma autoridade ou um organismo público, excetuando os tribunais no exercício da sua função jurisdicional."

de nomeação de um só Encarregado para várias autoridades públicas, como se fossem um “grupo empresarial”.

No caso das administrações tributárias, entendemos que, em razão da especificidade da função e a incidência de regime constitucional (como no caso de sigilo fiscal e bancário), isso levaria à necessidade de indicação de Encarregado próprio e autônomo, a fim de também manter a própria independência na atuação das administrações tributárias.

Ademais, a atividade de administração tributária envolve o tratamento de dados pessoais de todos os contribuintes da respectiva esfera federativa (seja União, Estado, Distrito Federal ou Município). Logo, o volume e a escala de tratamento é algo que justifica a nomeação de Encarregado próprio para as administrações tributárias, para que não haja acúmulo de funções ou conflito de interesses caso não seja exclusivo para essa finalidade.

2.5.3. Monitoramento fiscal do contribuinte

No que se refere ao controle de acesso em relação aos dados pessoais, como ventilado,[37] o monitoramento se faz presente e é peça importante para o controle de acesso a tais informações. Isso porque acessos não autorizados ou indevidos podem expor titulares de dados pessoais de maneira indevida, sobretudo em questões relativas a sigilo fiscal.

Logo, é inconteste que o monitoramento deve ser uma prioridade no seio da administração pública:

> Quando monitoramos uma plataforma de armazenamento de dados, queremos, na verdade, identificar rapidamente a ação. No caso de um evento de alteração, queremos saber o que foi alterado, quem alterou, quando aconteceu, de onde partiu o acesso que permitiu a alteração e tudo o que estiver relacionado com esse tipo de evento. Devemos ainda ter a possibilidade de gerar relatórios automatizados mensalmente ou semestralmente para certas ações de tratamento de dados, como coleta,

[37] Ver item 1.2.1.

> classificação, armazenamento, modificação, entre outras, e não somente ter a visibilidade de como estamos tratando. [...]" (DONEDA, 2020, p. 77)

Um ponto relevante no que se refere ao tratamento de dados pessoais em grande volume é o chamado **monitoramento fiscal**, que é corolário da própria atividade tributária. Atualmente, com o agigantamento do uso da Internet e a maior complexidade das relações sociais – e, outrossim, das relações tributárias –, é natural que as administrações tributárias passem a monitorar alguns ambientes para tentar extrair signos de riqueza dos contribuintes, principalmente nos meios digitais. Nesse sentido, o meio virtual é um importante depositário de provas virtuais[38] para as autoridades tributárias.

A maior questão do monitoramento fiscal é que ele geralmente se vale do uso de informações sem que o titular de dados tenha conhecimento de que está sendo monitorado, o que pode gerar certa controvérsia jurídica em sua aplicação. Muito comum, por exemplo, é o uso de redes sociais para esse monitoramento: quando um contribuinte publica alguma informação sobre algum bem não declarado, isso pode chamar a atenção das autoridades tributárias. Como não há nenhuma orientação específica a respeito desse tipo de fiscalização, ela pode ocorrer de maneira aleatória por parte do auditor responsável, conforme destaca LIMA (2015).

Portanto, o que seria fundamental é que a transparência no tratamento de dados pessoais pudesse, ao menos, deixar claro ao contribuinte que esse monitoramento fiscal com base em dados pessoais publicados na internet estaria

---

[38] "São fatos ocorridos por meio digitais e a respeito dos quais a prova pode ser feita (prova digital), por exemplo: envio de um **e-mail**, envio de uma mensagem por aplicativo de mensagens (WhatsApp, Telegram, entre outros), cópia ou desvio da base de dados, cópia de **software**, disponibilização de um vídeo na internet (conteúdo íntimo ou difamador), entre outros. Também é possível que o meio digital sirva de instrumento para demonstrar a existência de um fato ocorrido em meio não digital.
[...]
Dito isso, somando-se às ideias postas até aqui, parece ser possível conceituar a prova digital como: o instrumento jurídico vocacionado a demonstrar a ocorrência ou não de determinado fato e suas circunstâncias, tendo ele ocorrido total ou parcialmente em meios digitais ou, se fora deles, esses sirvam como instrumento para sua demonstração. A prova digital é o meio de demonstrar a ocorrência de um fato ocorrido em meio digital, ou que tem no meio digital um instrumento de demonstração de determinado fato de seu conteúdo." (THAMAY; TAMER, 2020, pp. 32-33)

ocorrendo. Muitos contribuintes são surpreendidos com tal fato, na ilusão de que a rede social, estando configurada como “privada” e restrita para poucas pessoas, não haveria monitoramento por parte de autoridades.

A preocupação não é exclusiva no cenário brasileiro, tendo havido discussões a respeito também na França:

> Na seara tributária, reconhecemos atividade de tratamento de dados pelo poder público nos casos vinculados à fiscalização do contribuinte, sendo cada vez mais frequente a atividade de monitoramento e tratamento de dados e informações de redes sociais de contribuintes pela Receita Federal. O monitoramento de redes sociais é um indício que se soma a outros cruzamentos efetuados por seus auditores, tais como movimentações financeiras, fontes pagadoras, veículos, entre outros.
>
> Procedimentos semelhantes vêm sendo utilizados pelo Fisco de outros países. Em recente decisão do Tribunal Constitucional da França, o fisco francês foi autorizado a revisar perfis, postagens e fotos de contribuintes para comprovar eventual renda não declarada. A decisão do Tribunal reconheceu que a privacidade e a liberdade de expressão dos usuários poderiam ser comprometidas com essa medida e recomendou a aplicação da legislação com ressalvas, estabelecendo limitações sobre quais informações podem ser coletadas, ressaltando que somente as informações públicas podem ser utilizadas pelo Fisco (SERAFINO, 2020, p. 251-252).

Logo, o Tribunal Constitucional da França parece ter decidido não proibir o uso de monitoramento de dados pessoais para fins fiscais, desde que os direitos dos contribuintes sejam preservados, em especial com a informação do que pode e do que não pode ser usado pelo fisco. Essa linha de raciocínio poderia ser aplicada no Brasil.

A LGPD, em essência, prescreve as obrigações de informação ao titular no artigo 9º, as quais são as mesmas para os setores público e privado. Portanto, entendemos que a LGPD já abrigaria essa necessidade de que as informações estejam amplamente disponíveis caso a autoridade fazendária realize tratamento de dados pessoais para fins de monitoramento fiscal.

Nesse contexto de monitoramento, ganha força o uso de inteligência artificial e outros mecanismos de ciência de dados para que esse acompanhamento

seja potencializado e que as informações mais importantes para fins fiscalizatórios sejam filtradas e passadas para uma análise humana:

> E, ao final, deveríamos reconhecer que se está a atribuir um poder extremamente importante à máquina, aquele de selecionar quais os erros que ela revela serem mais significativos e que mereceriam a atenção especial do agente aduaneiro – portanto, quando ela decide tudo o que merece ser fiscalizado, também decide tudo o que não merece atenção do Estado. Ao contrário do que possa parecer, o poder da máquina está justamente em decidir o que **não** deve ser fiscalizado.
>
> [...]
>
> Portanto, sabendo que o sistema é capaz de calcular inclusive o que ele chama de **expectativa de perda** – que, ao contrário da **expectativa de retorno**, corresponde a possibilidade de que a verificação acabe apurando diferenças tributárias favoráveis ao contribuinte -, não seria juridicamente correto dizer que uma verificação dessa natureza causaria **prejuízo** à Administração Fazendária. (KÖCHE, 2021, p. 194)

O problema das decisões automatizadas foi disciplinado no artigo 20 da LGPD, trazendo o direito do titular de solicitar a revisão de decisões tomadas somente com base em tratamento automatizado que possam afetar seus interesses. O parágrafo primeiro determina que o controlador tem de fornecer informações sobre os critérios e os procedimentos utilizados para a decisão automatizada, ressalvando a importância do respeito aos segredos comercial e industrial.

Percebe-se que esse dispositivo foi pensado para fins privados, sobretudo nas decisões que tratam de crédito pessoal. Não raro, as empresas estão automatizando essas decisões com base em algoritmos, dado o volume de solicitações diárias por parte de clientes.

No que se refere ao setor público, poderia haver algum parágrafo ou dispositivo específico que trouxesse à disciplina decisões automatizadas no âmbito dessa seara, visto que podem ser a fundamentação de um ato administrativo que implique restrições de direitos ao cidadão – como a aplicação de uma multa tributária.

Para que o monitoramento possa ser objeto de controle (o *accountability* previsto no artigo 6º, X da LGPD), é importante que o Encarregado mantenha o registro das operações de tratamento, conforme determinado no artigo 37 da LGPD. Para tanto, convém destacar a definição do que vem a ser registro de operações de tratamento, conforme descreve FURTADO (2020, pp. 87-88):

> Pela definição descritiva, temos que o registro de operações de dados pessoais é a compilação estruturada de informações relacionadas às operações de tratamento de dados pessoais, coletadas por meio de tarefas de mapeamento de dados (*Data Mapping*) e/ou mediante ferramentas de descobrimento de dados (*Data Discovery*).
>
> Por sua vez, o *data mapping* pode ser definido como uma atividade de catalogação de todo o fluxo de dados pessoais que são objeto de qualquer operação de tratamento [...] por uma organização, bem como os seus principais elementos (quais são os tipos de dados, formato, finalidade, base legal, localização etc.). O *data mapping* é realizado mediante entrevistas ou preenchimento direto de formulários (*self-assessment*).
>
> De outro lado, o *Data Discovery* pode ser definido como um processo realizado a partir da combinação de ferramentas e processos de *software*, com objetivo de identificar quais são os dados objeto de tratamento organização, seja aqueles armazenados em suas instalações, ou na nuvem, em redes de parceiros e repositórios externos, ou nos dispositivos pessoais de sua equipe. Essas ferramentas podem identificar quaisquer dados mantidos em qualquer formato, como documentos, apresentações e *e-mails*.

Por fim, o monitoramento fiscal caminha *pari passu* com o cuidado que as autoridades tributárias devem ter na parte operacional em relação aos dados pessoais, reforçando o ponto destacado anteriormente da importância de um programa de governança em privacidade do artigo 50, aplicável sobretudo ao poder público.

2.6. Normas específicas na proteção de dados pessoais no direito público brasileiro: o caso da MP nº 954/2020

Em linha com a crítica feita anteriormente[39] sobre a terminologia “geral”, é de se imaginar que a LGPD possa justamente servir como “norma-base” em matéria de proteção de dados pessoais, abrindo espaço para normas específicas regulamentarem pontos não enfrentados da LGPD, em especial nos aspectos de direito público[40].

O próprio artigo 4º, inciso III, da LGPD prescreve que o tratamento de dados pessoais para fins de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais não estão sujeitos à LGPD. Em suma, a própria norma reconhece que não é uma regulamentação fechada em si mesmo, exigindo detalhamentos de pontos específicos, seja expressa, como neste caso, ou tacitamente.

Com o advento da pandemia de Covid-19 e todas as suas consequências sanitárias, econômicas e sociais, houve um maior recrudescimento das questões relativas à privacidade dos cidadãos e, por consequência, o uso dos dados pessoais.

A excepcionalidade da situação motivou governos no mundo inteiro a cruzar diversas “linhas cinzentas” em relação à privacidade *versus* o direito à saúde dos indivíduos. No mundo todo foram introduzidas medidas de monitoramento por geolocalização, reconhecimento facial e aferição de temperatura em lugares públicos, bem como outras tecnologias, como forma de frear o alastramento do vírus.

No Brasil, a legislação seguiu nesta linha. Em primeiro lugar, houve a promulgação da chamada “Lei do Covid”, a Lei nº 13.979/2020, a qual dispõe sobre as medidas para o enfrentamento da pandemia. O artigo 6º, por exemplo, deixa explícita a obrigação de compartilhamento de dados pessoais a respeito de pessoas infectadas pelo SARS-CoV-2:

---

[39] Ver item 1.3.3.

[40] Aqui houve o cuidado de não se denominar **norma geral** para não causar confusão em relação à competência da União para estabelecer normas gerais no artigo 24 da Constituição da República Federativa do Brasil, tal como debatido no primeiro capítulo deste trabalho.

> Art. 6º É obrigatório o compartilhamento entre órgãos e entidades da administração pública federal, estadual, distrital e municipal de dados essenciais à identificação de pessoas infectadas ou com suspeita de infecção pelo coronavírus, com a finalidade exclusiva de evitar a sua propagação.
>
> § 1º A obrigação a que se refere o caput deste artigo estende-se às pessoas jurídicas de direito privado quando os dados forem solicitados por autoridade sanitária.
>
> § 2º O Ministério da Saúde manterá dados públicos e atualizados sobre os casos confirmados, suspeitos e em investigação, relativos à situação de emergência pública sanitária, resguardando o direito ao sigilo das informações pessoais

Percebe-se, portanto, que a legislação começou a avançar diretamente em questões relativas a dados pessoais, causando muita preocupação nos operadores do direito. Para tanto, o controle jurídico do que estava sendo emitido para o combate à pandemia passou a ser mais intenso por parte dos estudiosos de proteção de dados e também dos tribunais brasileiros.

O melhor exemplo em relação a esse controle deu-se em razão do advento da Medida Provisória nº 954/2020. Essa MP tinha como objetivo o compartilhamento de dados pessoais de usuários por parte das prestadoras de serviços de telecomunicações com o Instituto Brasileiro de Geografia e Estatística (IBGE). Com isso, ter-se-ia a possibilidade de construir uma estatística oficial durante a pandemia, dentro das limitações de distanciamento social exigidas para seu combate.

Em essência, a MP tinha como obrigação que as empresas de telefonia fixa e móvel disponibilizassem ao IBGE nomes, números de telefone e endereços de todos os cidadãos consumidores, pessoas físicas ou jurídicas. Embora a LGPD não se aplique diretamente no segundo caso (porém, há aplicação indireta, já que são tratados dados pessoais dos representantes legais), no primeiro caso seu impacto é direto.

Da posse desses dados, o IBGE poderia produzir sua estatística oficial utilizando entrevistas domiciliares no formato remoto. Logo, o IBGE passou a notificar as empresas sujeitas para que fornecessem essas informações o quanto antes.

A MP propunha algumas medidas acessórias, como o tratamento sigiloso dos referidos dados, bem como vedação expressa ao compartilhamento das informações a outras entidades da administração pública e empresas privadas. Também dispunha que o IBGE divulgaria, em seu site quando necessário, o relatório de impacto à proteção de dados pessoais. E, com o fim da situação emergencial, os dados seriam eliminados de suas bases de dados.

No entanto, o texto da MP não foi bem recebido no seio da comunidade jurídica e houve a propositura de cinco Ações Diretas de Inconstitucionalidade (ADIs) por diversos legitimados para contestar essas novas regras: (i) Conselho Federal da Ordem dos Advogados do Brasil – OAB (ADI 6.387), (ii) Partido da Social Democracia Brasileira – PSDB (ADI 6.388), (iii) Partido Socialista Brasileiro – PSB (ADI 6.389), (iv) Partido Socialismo e Liberdade – PSOL (ADI 6.390) e (v) Partido Comunista do Brasil (ADI 6.393).

Em todas elas, os argumentos são semelhantes, pugnando pela inconstitucionalidade formal e material da MP. A inconstitucionalidade formal viria em decorrência do desrespeito ao comando do artigo 62, *caput*, da Constituição da República Federativa do Brasil. As ADIs alegam que não ficou evidenciado, pelo Poder Executivo, o cumprimento dos requisitos da relevância e urgência que permitisse a edição da referida MP.

No que se refere à inconstitucionalidade material, haveria violação dos dispositivos da Constituição da República Federativa do Brasil que asseguram a dignidade da pessoa humana, a inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas, o sigilo dos dados, entre outros postulados inscritos constitucionalmente.

Ao analisar as referidas ADIs, a Ministra Relatora Rosa Weber deferiu na ADI 6.387, em decisão monocrática cautelar *ad referendum*[41] – que depois se confirmou no plenário do Supremo Tribunal Federal (por 10 votos a 1, vencido o Ministro Marco Aurélio Mello)[42] –, para suspender sua eficácia e determinar, como consequência, que o IBGE se abstivesse de requerer a disponibilização dos dados pessoais e, caso já o tivesse feito, que fosse sustado tal pedido, com imediata comunicação à respectiva operadora de telefonia.

[41] Em 24 de abril de 2020.
[42] Em 7 de maio de 2020.

Como argumento, a Ministra Relatora consignou que a Constituição da República Federativa do Brasil traria proteção especial à intimidade, à vida privada, à honra e à imagem das pessoas ao qualificá-las como invioláveis, como direitos fundamentais da personalidade, garantindo indenização pelo dano material ou moral decorrente de sua violação (art. 5º, X). Concluiu, assim, que o direito à privacidade (bem como os seus direitos decorrentes à intimidade, à honra e à imagem) surgem do próprio reconhecimento de que a personalidade individual deve ser protegida em todas as suas manifestações, não cabendo ao Estado tolhê-la.

Ficou consignado também que os dados pessoais disciplinados na MP estão no âmbito de proteção constitucional (artigo 5º) que tutela o direito à intimidade, à vida privada, à honra e à imagem das pessoas. A Ministra ressaltou que a MP não vislumbrou a exigência de mecanismos e de procedimentos para assegurar o sigilo, a higidez e o anonimato dos dados pessoais objeto de uso compartilhado, o que não atende às exigências estabelecidas na Constituição da República Federativa do Brasil para que exista a proteção de direitos fundamentais dos cidadãos.

A Ministra salientou que os dados de nomes, números de telefone e endereços dos consumidores dos serviços de telefonia são pessoais e estão contidos no âmbito de proteção das disposições constitucionais assecuratórias da liberdade individual (art. 5º, caput), da privacidade e do livre desenvolvimento da personalidade (art. 5º, X e XII).

Aqui convém destacar os comentários de GASIOLA, MACHADO e MENDES (2021, pp. 143-144) sobre essa tendência da Corte no que se refere à interpretação do dispositivo:

> Nos últimos julgamentos do STF a respeito das informações pessoais, nota-se uma ampliação do âmbito de proteção constitucional aos titulares de dados pessoais. Em especial, o entendimento restritivo do inciso do art. 5º, XII, da CF, pelo qual a inviolabilidade protegeria apenas os dados em comunicação, parece ter sido superado com o reconhecimento da inviolabilidade também aos dados pessoais de forma geral, bem como dos dados armazenados. Nota-se que a jurisprudência do STF está em rápida evolução nesse tema (ADPF 695 – Caso Abin/Denatran; ADI 656 - Cadastros de dependentes químicos e ADI 6.529 – Caso Sisbin), tendo tido em 2020 importantes julgados que certamente influenciarão toda a temática da proteção de dados nos próximos anos.

> Entre os julgados, merece especial destaque o caso IBGE (ADIs n. 6387, 6388, 6389, 6390 e 6393), no qual o STF reconheceu que o direito à proteção de dados tem *status* de direito fundamental, o que traz importantes impactos para o tratamento de dados na Administração Pública. Isso importa na ampliação do âmbito de proteção de qualquer informação relacionada a pessoas naturais, independentemente de uma relação direta com a vida privada, intimidade, imagem ou honra. Assim, qualquer tratamento de dados pessoais será objeto de proteção como elemento imprescindível à garantia de um direito geral de personalidade.

A Ministra ressaltou ainda que o respeito à privacidade e à autodeterminação informativa, decorrências dos direitos da personalidade, foram insculpidos no art. 2º, incisos I e II, da LGPD, ganhando o status de fundamentos específicos da disciplina da proteção de dados pessoais no Brasil. Com isso, foi a primeira decisão constitucional de relevância que aplicou a LGPD, mesmo ainda no período de *vacatio legis*.

A Ministra também pontuou que não há interesse público legítimo no uso compartilhado dos dados pessoais dos usuários dos serviços de telefonia. Ademais, a MP não ofereceu condições para avaliação da adequação e da necessidade de tais dados, pois não define a forma e a finalidade da utilização dos dados pessoais em questão.

Aqui se percebe que a Ministra Rosa Weber se vale ostensivamente de princípios da LGPD introduzidos no artigo 6º, como finalidade, adequação e necessidade, para fundamentar os tratamentos de dados pessoais em questão. Também se conecta com o artigo 10, que trata do legítimo interesse, para a hipótese aventada. Não é correta a correlação entre o legítimo interesse sob o aspecto técnico da LGPD com a hipótese em questão, pois ela mais se aproxima da verificação de um interesse público primário a motivar tal uso compartilhado, e não nas hipóteses trazidas pela norma para fundamentar o legítimo interesse.

Em continuação ao uso dos conceitos do artigo 6º da LGPD, a Ministra afirmou que, ao não se definir apropriadamente como e para que serão utilizados os dados pessoais, a MP não reúne condições para avaliação de sua adequação e necessidade, assim entendidas como a compatibilidade do tratamento com as finalidades informadas e sua limitação ao mínimo necessário para alcançar as respectivas finalidades.

Ademais, apontou que a MP não apresenta mecanismo técnico ou administrativo apto a proteger os dados pessoais de acessos não autorizados, vazamentos acidentais ou utilização indevida, seja na transmissão ou no tratamento. Isso significa que na parte de segurança da informação, ela não reúne disposições suficientes para trazer a tranquilidade de que os dados pessoais serão tratados de maneira segura pelo IBGE.

Esse ponto é de especial atenção, pois, como se ressaltou neste trabalho, o setor público brasileiro foi vitimado por números recordes de ataques cibernéticos. E, virtualmente, a MP permitia que o IBGE construísse uma base de dados pessoais valiosíssima para exploração por pessoas mal-intencionadas, o que exigia maior disciplina a respeito do tema.

Quanto a esse aspecto, conclui a Ministra que a MP apenas delega a ato do Presidente do IBGE o procedimento para uso compartilhado dos dados, sem que haja proteção suficiente aos direitos fundamentais em questão. Por fim, ela ressaltou que havia gravidade e urgência decorrente da atual crise sanitária, sendo necessária a formulação de políticas públicas para o enfrentamento do novo coronavírus, ainda que essas demandem dados pessoais dos cidadãos. No entanto, avaliou que o combate à pandemia não pode legitimar “o atropelo de garantias fundamentais consagradas na Constituição”.

A análise do caso faz-se pertinente ao objeto deste trabalho porque o controle de constitucionalidade feito pela Corte demonstrou que o setor público não pode ser visto como uma entidade excepcional ao tratar os dados pessoais, devendo, portanto, se submeter aos comandos da LGPD. Isso é particularmente interessante, pois mesmo com a edição de uma MP específica (que tem força de lei), os postulados da LGPD, como uma espécie de norma-base sobre dados pessoais, acabaram prevalecendo. Em especial, cumpre sublinhar o destaque dado ao princípio da finalidade na decisão.

O principal ponto que convém destacar em uma análise crítica do conteúdo da MP 954/2020 é que sequer era necessária a edição desse tipo de ato normativo por parte da Presidência da República, de natureza transitória, considerando que a LGPD já poderia dar solução jurídica para o tratamento de dados pessoais que o IBGE necessitava para seus misteres, bastando um ato infralegal a respeito.

A LGPD prevê extensivamente a hipótese de uso compartilhado de dados pessoais entre entes públicos e privados. Inclusive, o artigo 7º, inciso III, seria a base normativa para o tratamento desses dados pessoais pelo IBGE, sendo necessário convênio ou instrumento congênere de acordo administrativo entre as partes, sem necessidade de lei específica. Nesse caso, seria suficiente que as empresas de telefonia atualizassem os titulares a respeito das informações sobre o uso compartilhado, como demanda o artigo 9º, inciso V, da própria LGPD.

As restrições acerca do uso compartilhado de dados pessoais descritos no artigo 26, § 1º, da LGPD são relativas ao vetor "público-privado" no fluxo dos dados pessoais, e não o "privado-público". Considerando que o setor de telecomunicações possui regulação específica, seria necessário apenas um ato normativo de seu respectivo regulador, a Agência Nacional de Telecomunicações – ANATEL, que permitisse esse compartilhamento no vetor "privado-público".

Ademais, a própria ANPD, que à época não havia sido criada pelo Governo Federal por conta de sua própria inércia[43] administrativa, poderia regulamentar especificamente esse tema, conforme descreve o artigo 30 da LGPD. A regulamentação das atividades de comunicação e o uso compartilhado de dados pessoais continua inclusive sem regulamentação específica da autoridade até a presente data.

Por conseguinte, a edição da MP 954/2020 foi um erro de natureza política e jurídica, pois se utilizou de um meio desnecessário para o atingimento da finalidade almejada (uso de uma MP em vez de atos normativos infralegais). Com o rechaço pelo Poder Judiciário no que se refere a seu mérito, houve uma perda de oportunidade ao Governo Federal de que esse tema pudesse ser mais bem regulamentado infralegalmente, trazendo as salvaguardas técnicas e administrativas adequadas no que se refere à privacidade dos titulares a fim de não inquinar a norma de inconstitucionalidade. Nesse sentido, é importante destacar o papel relevante do Poder Judiciário nesse processo, resguardando os direitos fundamentais dos titulares e exaltando a própria democracia, conforme dizeres de ROCHA e UNES PEREIRA (2021a, p. 23).

[43] Tendo ocorrida a aprovação de sua estrutura regimental somente com o Decreto nº 10.474, de 26 de agosto de 2020, ou seja, na mesma data em que o Governo Federal teve ciência de que a MP nº 959/2020 não seria convertida em lei naquilo que se referia à extensão da vigência da LGPD.

Outra perda de oportunidade foi a possibilidade de ter regulado o uso compartilhado de dados na direção privado-pública, o que poderia ser útil para outros objetivos, como o tratamento de dados pelas autoridades tributárias.

2.7. Uma "LGPD Tributária" *de lege ferenda*?

Todo o debate em relação à insuficiência da LGPD no que se refere à disciplina de tratamento de dados vem motivando normas específicas para o tema, tal como a MP 954/2020 e o anteprojeto da chamada "LGPD Penal", que tramita na Câmara dos Deputados, que disciplina o tratamento de dados pessoais para fins de segurança pública (COSTA; REIS, 2021).

Nesse sentido, é possível que surja uma profusão de proposituras e normas jurídicas específicas a reger o tratamento de dados no setor público em algumas searas. Seria possível, portanto, conceber-se, nesse contexto, uma espécie de "LGPD Tributária"?

Ao analisar o posicionamento de SEER (2020), é possível verificar que o direito alemão compatibilizou o AO com o GDPR, sem necessidade de emissão de normas específicas para disciplinar o tratamento de dados pessoais para fins fiscais. O fato é que o direito tributário brasileiro também pode ir nessa vertente, considerando que o Código Tributário Nacional é uma norma geral de direito tributário, sendo recepcionada com o *status* de lei complementar (dentro da exigência do artigo 146, III, da Constituição da República Federativa do Brasil) e que baliza a atividade de administração tributária nos três níveis federativos.

Não faria sentido se falar de uma LGPD Tributária *de lege ferenda*, haja vista que alterações pontuais no próprio Código Tributário Nacional poderiam disciplinar questões relativas a tratamento de dados pessoais para fins fiscais, em especial para questões relativas ao monitoramento fiscal, compartilhamento de dados pessoais entre órgãos e entidades públicas para fins tributários e critérios para cumprimento do princípio da transparência insculpido no artigo 6º, VI, da LGPD.

Portanto, o melhor caminho seria uma harmonização da legislação tributária com a LGPD, e não a criação de uma lei específica para o tema, movimento que tem se demonstrado uma tendência com os exemplos da MP 954/2020 e a LGPD Penal. Um movimento disruptivo da legislação tributária em relação ao tratamento de dados pessoais, com uma lei específica e que não esteja em consonância com o sistema tributário brasileiro, poderá gerar dificuldade na parte da arrecadação tributária e, igualmente, insegurança jurídica – tanto para os fiscos como para os contribuintes.

Nesse sentido, algumas alterações pontuais no Código Tributário Nacional para harmonizar com a LGPD poderiam ser feitas, em especial no Título IV, que trata da administração tributária. Entre tais alterações, é possível ressaltar as discussões ventiladas até então:

> (i) Proibição de uso compartilhado de dados pessoais das autoridades tributárias com partes privadas que tenham como objeto social tratamento de dados pessoais para fins econômicos;
>
> (ii) Proteção ao segredo comercial e industrial de maneira explícita quando envolver o tratamento de dados pessoais, em consonância às ressalvas constantes feitas na LGPD sobre o tema;
>
> (iii) Proibição de tratamento de dados pessoais que estejam sujeitos a sigilo fiscal ou bancário para fins não tributários – exceto nos casos previstos em lei específica ou autorização judicial, como no caso de repressão a infrações penais (um exemplo é o caso de suspeitas de lavagem de dinheiro);
>
> (iv) Explicitação das finalidades de uso de dados pessoais nas atividades de arrecadação tributária, nas páginas virtuais das administrações tributárias, com a possibilidade de o contribuinte exercer seus direitos em relação a isso, incluindo o direito de

oposição caso o tratamento de dados para fins fiscais seja ilícito, por exemplo[44];

(v) Avisos recorrentes em relação à possibilidade de monitoramento fiscal por parte das autoridades tributárias em relação a dados pessoais de acesso público, como redes sociais, por exemplo;

(vi) Necessidade de nomeação de Encarregado de Proteção de Dados Pessoais específico e exclusivo para cada uma das administrações tributárias nos diversos entes federativos.

Por conseguinte, não seria necessária uma lei específica, uma "LGPD Tributária", para que as atividades de arrecadação e administração tributária estivessem em consonância com os princípios de preservação da privacidade e proteção de dados pessoais insculpidos na LGPD e – muito provavelmente em um futuro próximo – também na Constituição da República Federativa do Brasil, com a aprovação da PEC nº 17/2019.

[44] Por exemplo, caso a autoridade tributária "compre" uma base de dados privadas para poder exercer as atividades de exação tributária.

Conclusão

Esta dissertação profissional procurou demonstrar a incipiente tutela jurídica da proteção de dados pessoais no Brasil e seu impacto nas atividades do setor público, em especial nas administrações tributárias.

O direito à privacidade no Brasil é resguardado constitucionalmente pelo artigo 5º, inciso X, da Constituição da República Federativa do Brasil; contudo, a proteção de dados pessoais não possui a mesma estatura constitucional, o que vem motivado movimentos legislativos para essa finalidade, tal como a PEC nº 17/2019.

O grande marco normativo infraconstitucional em relação ao tema adveio com a figura da LAI, em 2011. A partir daí, houve uma profusão de normas sobre o tema, culminando na mais recente LGPD, em 2018. A construção normativa feita pela LAI em 2011 e pelo MCI em 2014 foram fundamentais para a gestação de uma cultura de maior responsabilidade em relação ao tratamento de dados pessoais no Brasil. Sem essas normas, arrisca-se afirmar que não haveria o terreno apropriado para que a LGPD pudesse ter o impacto e a efetividade que se espera no país.

Um dos aspectos importantes dessas duas normas, por exemplo, é o delineamento dos primeiros conceitos de dados pessoais, gestão do consentimento e eliminação de dados, bem como a disciplina jurídica de segurança da informação, que passou também a ser tratada infralegalmente em setores regulados, como no âmbito do Banco Central do Brasil e na CVM.

Com o surgimento da LGPD, houve o preenchimento de uma lacuna jurídica em relação ao tema. Porém, por se tratar de uma legislação muito inspirada na precedente europeia (o GDPR), que possui contexto específico, ela acabou sendo adaptada para a realidade nacional e, com isso, gerando algumas atecnias normativas – em especial disciplina dada ao setor público no que se refere ao tratamento de dados pessoais. Ademais, além de todas as discussões sobre o início da vigência da LGPD, que acarretou um atraso na sua entrada em vigor, existem muitas indefinições em relação aos conceitos jurídicos indeterminados lançados na norma.

Diante das atecnicas legislativas apontadas, a doutrina e jurisprudência terão papel crucial para dar contornos interpretativos a esses conceitos, a fim de trazer uma racionalização ao microssistema jurídico de privacidade e proteção de dados pessoais

A LGPD foi inovadora ao instituir um programa de governança em privacidade a fim de fazer valer seus fundamentos (artigo 2º) e princípios (artigo 6º) insculpidos na norma. Porém ela não deixa explícito se o setor público teria necessidade de estruturar o referido programa. Ocorre que, caso o setor público simplesmente ignore essas ferramentas de boas práticas e governança em privacidade e proteção de dados pessoais, os postulados da norma ficarão sujeitos a descumprimentos, haja vista a inexistência de qualquer ferramenta mitigante dos riscos envolvidos. Logo, entendemos ser importante que as administrações públicas também estruturem seus programas de governança em privacidade, pensando menos em eventual limitação de responsabilização e mais no descumprimento da própria norma.

Quando se aplicam os postulados de proteção de dados pessoais na atividade de tributação, acabam surgindo questões controvertidas de harmonização dessas duas searas do direito. Isso porque as normas de proteção de dados focam nas relações privadas, não se adentrando muito profundamente no influxo de regras e princípios de direito público nas relações entre Estado e sociedade.

Um exemplo é a questão do segredo comercial e industrial constantemente ressaltado na LGPD como ressalvas a algumas regras estabelecidas. Ocorre que, no direito tributário, o Código Tributário Nacional acaba não permitindo que se invoque tal circunstância contra o fisco, o que faz com que essas ressalvas da LGPD não se apliquem integralmente quando da atividade de arrecadação tributária. Isso poderia merecer um tratamento mais específico da norma.

Outrossim, as questões de sigilo fiscal e bancário, bem como também o uso compartilhado de dados pessoais dentro do próprio setor público, impõem severas restrições a alguns direitos do titular. Nesse sentido, a Receita Federal do Brasil editou recentemente o Manual Eletrônico do Sigilo Fiscal, a fim de resguardar essa garantia constitucional e legal dos contribuintes em relação a seus dados fiscais.

O uso compartilhado de dados pessoais não sujeitos a sigilo fiscal no setor público é a atividade em que há maiores riscos de violações aos direitos e garantias fundamentais trazidas na LGPD. Isso porque o potencial de que tais dados sejam utilizados para fins tributários é relevante, e a LGPD veio tratar especificamente sobre a finalidade de execução de políticas públicas e atribuição legal dos órgãos (artigo 26). Com o e-Social, por exemplo, em razão do volume de dados estruturados, começou-se a questionar as possibilidades de uso compartilhado com diversas administrações tributárias e consequentemente o risco de incidentes de segurança da informação que isso pode gerar.

No que se refere ao setor privado, a Receita Federal do Brasil, por meio da Portaria nº 4.255/2020, começou a limitar a disponibilização de dados pessoais para o mercado contidos na Nota Fiscal Eletrônica, trazendo importantes restrições às atividades econômicas de algumas empresas que se valem de dados pessoais como objeto-fim de sua atividade. Nessa mesma toada, cumpre destacar o veto ao artigo 29, § 3º, da Lei nº 14.129/2021, com semelhante teor.

Entendemos que negócios que têm como objeto social o tratamento intensivo de dados terão de se adaptar à LGPD e conceber formas mais criativas – e legais – para o tratamento de dados, evitando, por exemplo, a figura da "raspagem" ou outros métodos mais intrusivos à privacidade dos indivíduos.

A LGPD também originou alguns deveres das administrações tributárias em relação à proteção de dados pessoais. Segundo a LGPD, no artigo 6º, inciso I, todo tratamento deve ter uma finalidade específica, legítima, explícita e informada ao titular. Nesse sentido, o teste da finalidade deve abarcar a finalidade tributária, sem possibilidade de algum tipo de desvio de finalidade nesse ínterim. O princípio da finalidade na LGPD, portanto, ganha novo contorno com a administração pública: além da própria finalidade do tratamento, deve ser considerada a finalidade pública intrínseca aos atos administrativos na esfera tributária.

Outro direito do titular que se harmoniza com um dever ativo da administração é a transparência no que se refere às operações de tratamento, em especial o direito à informação em relação ao que é feito com os dados pessoais. Um ponto de câmbio na relação fisco-contribuinte vai ser a exacerbação da transparência quando a autoridade tributária estiver tratando dados para a sua

atividade, permitindo o direito de acesso às informações relativas ao tratamento de dados pessoais.

É certo que a autoridade tributária não poderá, de maneira preditiva, indicar quando estiver fazendo uma fiscalização ou algo similar, pois isso obstaria a própria atividade de arrecadação tributária. Mas posteriormente, em sede de defesa, o titular teria direitos de acesso aos dados pessoais para entender como foi feito o tratamento e, inclusive, fazer o controle de legalidade em relação ao tratamento realizado para fins tributários, o que em último grau poderia impactar até mesmo na legalidade da constituição do crédito tributário.

Aqui ganha força o uso do monitoramento fiscal, estratégia já utilizada pelas autoridades tributárias para coletar informações a respeito de bens ou rendas não declaradas pelo sujeito passivo da relação jurídica tributária. Como o titular geralmente não sabe que está sendo monitorado em relação a seus dados pessoais, entendemos que passará a ser um dever ativo de transparência das autoridades tributárias mencionar, sempre que possível, que dados pessoais com acesso público podem ser utilizados para esse fim.

Para garantir esses e outros deveres, será importante a figura do Encarregado de Proteção de Dados Pessoais no setor público, em especial um dedicado às autoridades tributárias, que fará os testes e as análises necessárias, produzindo inclusive o relatório de impacto à proteção de dados pessoais – artigo 5º, XVII, da LGPD.

Em razão de a LGPD ter sido uma norma não muito extensa ao disciplinar o tratamento de dados no setor público, é interessante começar a observar uma tendência de normas específicas, que, com supedâneo em uma espécie de norma "geral" como a LGPD, teriam o condão de disciplinar questões específicas de tratamento de dados pessoais no setor público.

O melhor exemplo é o estudo de caso da MP nº 954/2020, que veio a disciplinar o tratamento de dados pessoais pelo IBGE com o uso compartilhado de dados pessoais de empresas de telefonia. Em razão de a MP não ter esclarecido com detalhes como se dariam as salvaguardas em relação a esses tratamentos por parte do IBGE, acabou tendo sua eficácia suspensa por meio da apreciação da ADI 6.387 pelo Supremo Tribunal Federal.

Outro assunto que vem ganhando corpo nos debates legislativos é o anteprojeto da chamada “LGPD Penal”, a qual viria disciplinar os aspectos de tratamento de dados pessoais por parte das autoridades policiais e judiciárias para fins de persecução penal.

Logo, diante desse contexto, convém refletir se seria necessária uma “LGPD Tributária” como proposta *de lege ferenda*. Concluímos pela sua desnecessidade com base no caminho trilhado pela legislação tributária alemã, conforme exposto no trabalho de SEER. O que poderia ser proposto é a realização de alterações pontuais no Código Tributário Nacional de modo a contemplar princípios e regras específicas de tratamento de dados pessoais para fins tributários, trazendo algumas proibições às autoridades tributárias e maiores proteções ao contribuinte como titular de dados pessoais.

Bibliografia

ALMEIDA, Fernando Dias Menezes de; LINO, Fernanda Noia da Costa. Do uso compartilhado de dados pessoais pelo poder público. *In:* MONACO, Gustavo Ferraz de Campos; MARTINS, Amanda Cunha e Mello Smith; CAMARGO, Solano de (orgs.). **Lei Geral de Proteção de Dados: ensaios e controvérsias da Lei 13.709/18**. São Paulo: Quartier Latin, 2020, pp. 327-338.

ALVES, Fabrício da Mota. Desafios da adequação do Poder Público à LGPD. *In:* PALHARES, Felipe (coord.). **Temas atuais de proteção de dados**. São Paulo: Thomson Reuters Brasil, 2020a, pp. 171-196.

_____. Estruturação do cargo de DPO em entes públicos. *In:* BLUM, Renato Opice; VAINZOF, Rony; MORAES, Henrique Fabretti (coords.). **Data Protection Officer (Encarregado): teoria e prática de acordo com a LGPD e o GDPR**. São Paulo: Thomson Reuters Brasil, 2020b, pp. 523-544.

BAIÃO, Renata Barros Souto Maior; TEIVE, Marcello Muller. O artigo 23 da LGPD como base legal autônoma para o tratamento de dados pessoais pelo poder judiciário. *In:* PALHARES, Felipe (coord.). **Temas atuais de proteção de dados**. São Paulo: Thomson Reuters Brasil, 2020, pp. 303-319.

BARBIERI, Carlos. **Governança de dados: práticas, conceitos e novos caminhos.** Rio de Janeiro: Alta Books, 2019.

BATISTA, Diego Alves Amaral; RANGEL, Luís Felipe Vieira. Aspectos fiscais aplicáveis à cessão e disponibilização de dados. *In:* FARIA, Renato Vilela; SILVEIRA, Ricardo Maitto; MONTEIRO, Alexandre Luiz Moraes do Rêgo. **Tributação da economia digital: desafios no Brasil, experiência internacional e novas perspectivas**. São Paulo: Saraiva Educação, 2018, pp. 760-778.

BECHARA, Carlos Henrique Tranjan; CARVALHO, João Rafael L. Gândara de. Estado Democrático de Direito ou Estado Burocrático de Deveres? A Administração Tributária e o setor de telecomunicações nos 30 anos da Constituição Cidadã. *In:* ALVES, Gustavo Baptista *et al*. (coords.). **Tributação de novas tecnologias e telecomunicações**. São Paulo: Quartier Latin, 2019, pp. 93-112.

BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. 2ª ed. Rio de Janeiro: Forense, 2021.

BRASIL. Você sabe o que tem a ver Revolução Francesa e Acesso à Informação? **Ouvidorias.gov.** 18. Jul. 2018. Disponível em: <https://www.gov.br/ouvidorias/pt-br/assuntos/noticias/2018/voce-sabe-o-que-tem-a-ver-revolucao-francesa-e-acesso-a-informacao>. Acesso em: 7 jan. 2022.

CARVALHO, Paulo de Barros. **Curso de direito tributário**. 28ª ed. São Paulo: Saraiva, 2017.

CAVALIERI FILHO, Sérgio. **Programa de Responsabilidade Civil**. 12ª ed. São Paulo: Atlas, 2015.

CHAVES, Luis Fernando Prado. Responsável pelo tratamento, subcontratante e DPO. *In:* MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (coords.). **Comentários ao GDPR: Regulamento Geral de Proteção de Dados da União Europeia.** São Paulo: Thomson Reuters Brasil, 2018, pp. 111-138.

CHINELLATO, Silmara Juny de Abreu; MORATO, Antonio Carlos. Direitos básicos de proteção de dados pessoais, o princípio da transparência e a proteção dos direitos intelectuais. *In:* DONEDA, Danilo *et al.* (coords.). **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021, pp. 641-664.

COSTA, Eduarda; REIS, Carolina. Histórico da LGPD Penal: o que foi feito até aqui e quais são os próximos passos? **Lapin**. 16 abr. 2021. Disponível em: <https://lapin.org.br/2021/04/16/lgpd-penal-o-que-foi-feito-ate-aqui-e-quais-sao-os-proximos-passos/>. Acesso em: 07 jul. 2021.

COSTA, Regina Helena. **Curso de direito tributário**. 7ª ed. São Paulo: Saraiva, 2017.

CNNBRASIL. **Site do Ministério da Saúde sofre ataque hacker durante madrugada e sai do ar.** 10 dez. 2021. Disponível em: <https://www.cnnbrasil.com.br/nacional/site-do-ministerio-da-saude-sofre-ataque-hacker-durante-madrugada-e-sai-do-ar/>. Acesso em: 07 jan. 2022.

CURY, Antonio Alberto Rondina. A responsabilidade do Estado no tratamento de dados pessoais por órgãos públicos. *In:* MONACO, Gustavo Ferraz de Campos; MARTINS, Amanda Cunha e Mello Smith; CAMARGO, Solano de (orgs.). **Lei Geral de Proteção de Dados: ensaios e controvérsias da Lei 13.709/18**. São Paulo: Quartier Latin, 2020, pp. 135-142.

DI PIETRO, Maria Sylvia Zanella. **Direito administrativo**. 34ª ed. Rio de Janeiro: Forense, 2021.

DONDA, Daniel. **Guia prático de implementação da LGPD: conheça estratégias e soluções para adequar sua empresa em conformidade com a Lei**. São Paulo: Labrador, 2020.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais: elementos da formação da Lei Geral de Proteção de Dados.** 2ª ed. São Paulo: Thomson Reuters Brasil, 2019.

DRIGO, Leonardo Godoy. Distinção entre princípios e regras sob o critério da generalidade e abstração da norma jurídica no Brasil. **Revista Jus Navigandi**, ISSN 1518-4862. Teresina. ano 18, nº 3715. 2 set. 2013. Disponível em: <https://jus.com.br/artigos/25208>. Acesso em: 07 abr. 2021.

EXAME. **Vazamento de dados de "220 milhões de brasileiros" não aconteceu da noite para o dia**. 26 jan. 2021. Disponível em: <https://exame.com/tecnologia/vazamento-de-dados-de-220-milhoes-de-brasileiros-nao-aconteceu-da-noite-para-o-dia/>. Acesso em: 07 abr. 2021.

FALCÃO, Tatiana. Uma proposta para a modificação da Convenção Modelo da OCDE em face da digitalização da economia. *In:* FARIA, Renato Vilela; SILVEIRA, Ricardo Maitto; MONTEIRO, Alexandre Luiz Moraes do Rêgo. **Tributação da economia digital: desafios no Brasil, experiência internacional e novas perspectivas**. São Paulo: Saraiva Educação, 2018, pp. 944-958.

FEIGELSON, Bruno; WILSON, Andreu. Tratamento de dados pessoais pelo Poder Público. *In:* FEIGELSON, Bruno; BECKER, Daniel; CAMARINHA, Sylvia M. F. (coords.). **Comentários à Lei Geral de Proteção de Dados: Lei 13.709/2018.** São Paulo: Thomson Reuters Brasil, 2020, pp. 99-118.

FERNANDES, Edison Carlos. O que a declaração tributária tem a ver com a proteção de dados. **Migalhas de Peso**. 19 jun. 2019. Disponível em: <https://www.migalhas.com.br/depeso/304598/o-que-a-declaracao-tributaria-tem-a-ver-com-a-protecao-de-dados >. Acesso em: 7 abr. 2021.

FURTADO, Tiago Neves. Registro das operações de tratamento de dados pessoais – *data mapping* – *data Discovery*: por que é importante e como executá-lo. *In:* BLUM, Renato Opice; VAINZOF, Rony; MORAES, Henrique Fabretti (coords.). **Data Protection Officer (Encarregado): teoria e prática de acordo com a LGPD e o GDPR**. São Paulo: Thomson Reuters Brasil, 2020, pp. 85-104.

GARCIA, Lara Rocha *et al*. **Lei Geral de Proteção de Dados Pessoais (LGPD): guia de implantação**. São Paulo: Blucher, 2020.

GASIOLA, Gustavo Gil; MACHADO, Diego; MENDES, Laura Schertel. O tratamento de dados pessoais pela Administração Pública: transparência, bases legais e limites constitucionais. *In:* FRANCOSKI, Denise de Souza Luiz; TASSO, Fernando Antonio (coords.). **A Lei Geral de Proteção de Dados Pessoais LGPD: aspectos práticos e teóricos relevantes no setor público e privado**. São Paulo: Thomson Reuters Brasil, 2021, pp. 137-161.

GLASSMAN, Guillermo. Interfaces entre o dever de transparência e a proteção dos dados pessoais no âmbito da Administração Pública**.** *In:* DAL POZZO, Augusto Neves; MARTINS, Ricardo Marcondes (coords.). **LGPD & Administração Pública: uma análise ampla dos impactos**. São Paulo: Thomson Reuters Brasil, 2020, pp. 863-878.

GOMES, Daniel de Paiva *et al*. Os desafios impostos pela economia digital e o Plano de Ação 1 do Projeto BEPS da OCDE. *In:* PISCITELLI, Tathiane (org.); PISCITELLI, Tathiane; BOSSA, Gisele Barra (coords.). **Tributação da nuvem: conceitos tecnológicos, desafios internos e internacionais**. São Paulo: Thomson Reuters Brasil, 2018, pp. 43-66.

HINTZBERGEN, Jule *et al*. **Fundamentos de segurança da informação: com base na ISO 27001 e na ISO 27002.** Trad. Alan de Sá. Rio de Janeiro: Brasport, 2018.

KÖCHE, Rafael. A inteligência artificial a serviço da fiscalidade: sistema de seleção aduaneira por aprendizado de máquina (SISAM). *In:* MACHADO, Hugo de Brito (coord.). **Tributação e novas tecnologias**. São Paulo: Editora Foco, 2021.

LEONARDI, Marcel. **Fundamentos de direito digital**. São Paulo: Thomson Reuters Brasil, 2019.

LEORATTI, Alexandre. LGPD pode pressionar órgãos tributários no uso de dados dos contribuintes. **Jota**. 16 mar. 2021. Disponível em: <https://www.jota.info/tributos-e-empresas/tributario/lgpd-tributarios-contribuinte-16032021>. Acesso em: 1 maio 2021.

LIMA, Cíntia Rosa Pereira de; RAMIRO, Lívia Froner Moreno. Direitos do titular dos dados pessoais. *In:* LIMA, Cíntia Rosa Pereira de (coord.). **Comentários à Lei Geral de Proteção de Dados: Lei nº 13.709/2018, com alteração da Lei nº 13.853/2019.** São Paulo: Almedina, 2020, pp. 249-277.

LIMA, Rebeca. Receita Federal caça contribuintes 'pobres' nas redes sociais. **Jusbrasil**. 2015. Disponível em: <https://rebecaslima.jusbrasil.com.br/noticias/198324917/receita-federal-caca-contribuintes-pobres-nas-redes-sociais>. Acesso em: 1 maio 2021.

LOPES, Mariana Louback. Tratamento de dados pelo poder público. *In:* FEIGELSON, Bruno; SIQUEIRA, Antonio Henrique Albani (coords.). **Comentários à Lei Geral de Proteção de Dados: Lei 13.709/2018.** São Paulo: Thomson Reuters Brasil, 2019, pp. 135-146.

LÓSSIO, Claudio Joel Brito. **Proteção de dados e *compliance* digital.** São Paulo: Almedina, 2021.

MACHADO, Hugo de Brito. **Curso de direito tributário**. 40ª ed. São Paulo: Malheiros, 2019.

MARINHO, Fernando. **Os 10 mandamentos da LGPD: como implementar a Lei Geral de Proteção de Dados em 14 passos**. São Paulo: Atlas, 2020.

MICHAELIS. **Dicionário Brasileiro da Língua Portuguesa.** 2021. Disponível em: <https://michaelis.uol.com.br/>. Acesso em: 28 jun. 2021.

NETFLIX. **Privacidade hackeada**. Trad. do original "The Great Hack". Direção de Karim Amer, Jehane Noujaim. 24 jul. 2019.

_____. **O dilema das redes.** Trad. do original "The Social Dilemma". Direção de Jeff Orlowski. 9 set. 2020.

NOGUEIRA, Fernanda. **Reflexos da LGPD na área tributária**. 22 out. 2020. Disponível em: <https://www.fernandanogueira.com.br/post/reflexos-da-lgpd-na-área-tributária>. Acesso em: 07 abr. 2021.

PAULSEN, Leandro. **Curso de direito tributário completo**. 11ª ed. São Paulo: Saraiva Educação, 2020.

PEREIRA, Flávio Henrique Unes; CRUVINEL, Renan. A corregulação na Lei Geral de Proteção de Dados. **Blog Fausto Macedo, O Estado de São Paulo.** 3 dez. 2019.

OLIVEIRA, Ricardo; COTS, Márcio (coord.). **O legítimo interesse e a LGPD**. São Paulo: Thomson Reuters Brasil, 2020.

PINHEIRO, Patricia Peck. **Proteção de dados pessoais: comentários à Lei nº 13.709/2018 (LGPD)**. 2ª ed. São Paulo: Saraiva Educação, 2020.

POHLMANN, Sérgio. **LGPD ninja: entendendo e implementando a Lei Geral de Proteção de Dados nas empresas.** Nova Friburgo: Fross, 2019.

PUGLIESI, Márcio; GUNDIM, Wagner Wilson Deiró. A indeterminação semântica do conceito de dados pessoais cujo acesso é público/tornados públicos na Lei Geral de Proteção de Dados (LGPD) brasileira. *In:* MONACO, Gustavo Ferraz de Campos; MARTINS, Amanda Cunha e Mello Smith; CAMARGO, Solano de (orgs.). **Lei Geral de Proteção de Dados: ensaios e controvérsias da Lei 13.709/18**. São Paulo: Quartier Latin, 2020, pp. 491-498.

RAMOS, Cesar Augusto. Liberdade positiva e negativa no liberalismo político de Rawls. **Dissertatio**. UFPel, v. 34, 2011, pp. 253-281.

RECEITA FEDERAL DO BRASIL. Manual eletrônico do sigilo fiscal (e-MSF). 2020. Disponível em: <https://www.gov.br/receitafederal/pt-br/assuntos/orientacao-tributaria/sigilo-fiscal#:~:text=O%20Manual%20Eletr%C3%B4nico%20do%20Sigilo,judici%C3%A1rias%2C%20administrativas%2C%20e%20de%20terceiros>. Acesso em: 07 abr. 2021.

RIBEIRO, Giovana Bellini. Compatibilidade entre a proteção de dados pessoais e o dever de transparência pública. *In:* DAL POZZO, Augusto Neves; MARTINS, Ricardo Marcondes (coords.). **LGPD & Administração Pública: uma análise ampla dos impactos**. São Paulo: Thomson Reuters Brasil, 2020, pp. 293-309.

ROCHA, Fernando Clemente; UNES PEREIRA, Flávio Henrique. Democracia e jurisdição constitucional para a tutela de direitos fundamentais. *In:* DIAS, Maria Tereza Fonseca; UNES PEREIRA, Flávio Henrique (coords.). **O direito administrativo social e econômico: análises de direito comparado**. São Paulo: Almedina, 2021a, pp. 17-32.

_____. O (ainda) difícil diálogo entre Direito e Economia no Brasil. *In:* DIAS, Maria Tereza Fonseca; UNES PEREIRA, Flávio Henrique (coords.). **O direito administrativo social e econômico: análises de direito comparado**. São Paulo: Almedina, 2021b, pp. 109-118.

ROCHA, Henrique. Gestão de crises digitais, incidentes de segurança, comprometimento de dados pessoais e dados financeiros. *In:* CRESPO, Marcelo Xavier de Freitas (coord.). **Compliance no direito digital.** v. III. São Paulo: Thomson Reuters Brasil, 2020, pp. 219-233.

RODOTÀ, Stefano. **A vida na sociedade da vigilância: a privacidade hoje**. Trad. Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

SANTI, Danielle; MAFRA, Marcos Guilherme Rodrigues. A responsabilização da Administração Pública na Lei Geral de Proteção de Dados. *In:* PIRONTI, Rodrigo (coord.). **Lei Geral de Proteção de Dados no Setor Público**. Belo Horizonte: Fórum, 2021, pp. 137-150.

SENADO FEDERAL. **Lei Geral de Proteção de Dados entra em vigor**. 18 set. 2020. Disponível em: <https://www12.senado.leg.br/noticias/materias/2020/09/18/lei-geral-de-protecao-de-dados-entra-em-vigor>. Acesso em: 07 abr. 2021.

SCHOUERI, Luís Eduardo. **Direito tributário**. 9º ed. São Paulo: Saraiva Educação, 2019.

SEER, Roman. Proteção de dados e tributação na Alemanha: repercussões do Regulamento Geral sobre Proteção de Dados. **Revista Jurídica da Presidência**. Brasília, v. 22, n. 126, pp. 20-47, fev./maio 2020.

SHAH, Nidhi. **You Are Worth $182 To Google, $158 To Facebook And $733 To Amazon!,** s/d**.** Disponível em: <https://arkenea.com/blog/big-tech-companies-user-worth/>. Acesso em: 07 abr. 2021.

SERAFINO, Danielle Campos Lima. Direito tributário e tratamento de dados pelo poder público. *In:* BLUM, Renato Opice (org.). **Proteção de dados: desafios e soluções na adequação à lei**. Rio de Janeiro: Forense, 2020, pp. 241-256.

SILVEIRA, Milena. LGPD na prática: como a lei de dados pode afetar até a Receita Federal. **AG Capital**. 29 mar. 2021. Disponível em: < https://www.agcapital.com.br/ag-news/lgpd-na-pratica/>. Acesso em: 1 maio 2021.

TARTUCE, Flávio. **Manual de Direito Civil: volume único**. 11ª ed. Rio de Janeiro: Forense, 2021.

TASSO, Fernando Antonio. Capítulo IV: Do Tratamento de Dados Pessoais pelo Poder Público. *In:* MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (coord.). **LGPD: Lei Geral de Proteção de Dados comentada**. São Paulo: Thomson Reuters Brasil, 2019, pp. 245-285.

TEIXEIRA FILHO, Sócrates Arantes. **Segurança da informação descomplicada**. Brasília: Edição do Autor, 2015.

OLIVA, Milena Donato. **Teoria Geral do Direito Civil**. TEPEDINO, Gustavo (org.). Rio de Janeiro: Forense, 2020.

THAMAY, Rennan; TAMER, Mauricio. **Provas no direito digital: conceito de prova digital, procedimentos e provas digitais em espécie**. São Paulo: Thomson Reuters Brasil, 2020.

THE ECONOMIST. **The world's most valuable resource is no longer oil, but data**. 6 maio 2017. Disponível em: <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data>. Acesso em: 07 abr. 2021.

UNES PEREIRA, Flávio Henrique. **Regulação, fiscalização e sanção: fundamentos e requisitos da delegação do exercício do poder de polícia administrativa a particulares**. 2ª ed. Belo Horizonte: Fórum, 2020.

_____. **Sanções disciplinares: o alcance do controle jurisdicional**. 2ª ed. Belo Horizonte: Fórum, 2020.

_____; ALVIM, Rafael da Silva. Autorregulação na Lei Geral de Proteção de Dados e segurança jurídica. **Consultor Jurídico.** 27 out. 2020. Disponível em: <https://www.conjur.com.br/2020-out-27/pereira-alvim-autorregulacao-lgpd-seguranca-juridica>. Acesso em: 07 abr. 2021.

WARREN, Samuel D.; BRANDEIS, Louis D. The right of privacy. **Harvard Law Review**, vol. 4, nº 5. (15 dez. 1890), pp. 193-220.

WIMMER, Miriam. O regime jurídico do tratamento de dados pessoais pelo poder público. *In:* DONEDA, Danilo *et al.* (coords.). **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021, pp. 271-268.

XAVIER, Luciana Pedroso; XAVIER, Marília Pedroso; SPALER, Mayara Guibor. Primeiras impressões sobre o tratamento de dados pessoais nas hipóteses de interesse público e execução de contrato. *In:* TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (coord.). **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro**. 2ª ed. São Paulo: Thomson Reuters Brasil, 2020, pp. 479-498.

UOL. **Raspar o tacho: coleta maciça de todos nossos dados públicos virou "mina de ouro" de empresas, hackers e políticos.** 13 nov. 2020. Disponível em: <https://www.uol.com.br/tilt/reportagens-especiais/raspagem-de-dados-o-que-e-e-como-se-proteger/>. Acesso em: 07 abr. 2021.