UNIVERSIDADE FEDERAL DO MARANHÃO
CENTRO DE CIÊNCIAS SOCIAIS, SAÚDE E TECNOLOGIA
CURSO DE DIREITO

RAFAEL SOARES CRUZ

TRATAMENTO DE DADOS SIGILOSOS NO ÂMBITO FISCAL:
uma análise dos impactos da Lei Geral de Proteção de Dados na atuação da Receita Federal do Brasil

Imperatriz
2021

RAFAEL SOARES CRUZ

TRATAMENTO DE DADOS SIGILOSOS NO ÂMBITO FISCAL: uma análise dos impactos da Lei Geral de Proteção de Dados na atuação da Receita Federal do Brasil

Monografia apresentada ao Curso de Graduação em Direito da Universidade Federal do Maranhão como requisito para obtenção do Grau de Bacharel em Direito.

Orientadora: Prof.ª Dra. Ellen Patrícia Braga Pantoja

Imperatriz
2021

Ficha gerada por meio do SIGAA/Biblioteca com dados fornecidos pelo(a) autor(a).
Diretoria Integrada de Bibliotecas/UFMA

Cruz, Rafael Soares.
Tratamento de dados sigilosos no âmbito fiscal : uma análise dos impactos da Lei Geral de Proteção de Dados na atuação da Receita Federal do Brasil / Rafael Soares Cruz. - 2021.
73 f.

Orientador(a): Ellen Patrícia Braga Pantoja.
Monografia (Graduação) - Curso de Direito, Universidade Federal do Maranhão, Imperatriz, 2021.

1. Direito à privacidade. 2. Governança de dados pelo poder público. 3. Lei Geral de Proteção de Dados. 4. Receita Federal. 5. Sigilo fiscal e bancário. I. Pantoja, Ellen Patrícia Braga. II. Título.

Rafael Soares Cruz

TRATAMENTO DE DADOS SIGILOSOS NO ÂMBITO FISCAL: uma análise dos impactos da Lei Geral de Proteção de Dados na atuação da Receita Federal do Brasil

Monografia apresentada ao Curso de Graduação em Direito da Universidade Federal do Maranhão como requisito para obtenção do Grau de Bacharel em Direito.

Orientadora: Prof.ª Dra. Ellen Patrícia Braga Pantoja

COMISSÃO EXAMINADORA

_____

Prof.ª Dra. Ellen Patrícia Braga Pantoja – Orientadora

_____

Prof. Me. Denisson Gonçalves Chaves

_____

Prof.ª Ma. Francine Adilia Rodante Ferrari Nabhan

Imperatriz, MA, 20 de Maio de 2021.

AGRADECIMENTOS

Aos meus pais, Kedma e Artur, e irmãos, Gabriel, Fernando e Artur Filho, maiores motivadores na busca pelo permanente aperfeiçoamento.

À minha Lorena pelo carinho ilimitado que sempre oferece e pela paz que provoca em todos ao seu redor.

À amiga Marcella pelas críticas enriquecedoras e eterna discordância.

À professora Dra. Ellen Patrícia Braga Pantoja pela forma gentil e com extremo zelo com que guiou a construção do presente trabalho.

Aos colegas da turma de Direito pelo ambiente sempre rico em discussões que proporcionaram nesses anos de convivência acadêmica.

A todos os professores da Curso de Direito, pela disponibilidade em partilhar o seu saber.

Aos colegas da Receita Federal, profissionais da mais elevada capacidade técnica, por oferecerem um ambiente profissional sempre profícuo em aprendizados.

A constituição democrática é aquela que não apenas afirma as liberdades civis, porém cria os órgãos e as leis capazes de tornar estas liberdades efetivas e protegidas perante todos.

Norberto Bobbio

RESUMO

A Lei Geral de Proteção de Dados suscitou no direito brasileiro importante discussão sobre o tratamento de dados pessoais. Em razão disso, mostra-se importante analisar o impacto dessa Lei na atuação da Receita Federal, cujo trabalho baseia-se fortemente no tratamento de informações protegidas por sigilo. Diante dessa situação, o presente trabalho busca avaliar os impactos e consequências da edição de uma lei geral sobre a proteção de dados para o trabalho do Fisco Federal, avaliando de que modo o entendimento até então estabelecido sobre o tratamento de informações protegidas pelos sigilos fiscal e bancário é afetado pelo estabelecimento legal da disciplina de proteção de dados pessoais no ordenamento brasileiro. A pesquisa investiga o alcance da proteção de dados pessoais, partindo da discussão internacional sobre o direito à privacidade e chegando à atuação da Receita Federal após a edição da Lei, com análise de casos específicos recentes e pesquisa bibliográfica, de leis e de jurisprudências. O trabalho percorre a discussão em torno da tutela de dados pessoais, analisa os principais dispositivos da nova Lei e estuda a legislação e jurisprudência que orientam o tratamento de informações protegidas pelo sigilo fiscal e bancário, situando a nova Norma na discussão. Sua edição se soma às normas e jurisprudências existentes e estabelece a ampla proteção dos dados pessoais, fortalecendo o uso que a Administração Tributária Federal faz de informações sigilosas no cumprimento de sua competência legal.

Palavras-chave: Direito à privacidade; Lei geral de proteção de dados; Receita federal; Sigilo fiscal e bancário; Governança de dados pelo poder público.

ABSTRACT

The General Data Protection Law raised in Brazilian law an important discussion about the processing of personal data. As a result, it is important to analyze the impact of this Law on the work of the Federal Revenue Service, whose work is strongly based on the treatment of information protected by secrecy. Given this situation, the present study seeks to assess the impacts and consequences of editing a general law on data protection for the work of the Federal Tax Authority, assessing how the previously established understanding about the treatment of information protected by fiscal and banking secrecy is affected by the legal establishment of the discipline of protection of personal data in the Brazilian legal system. The research investigates the scope of the protection of personal data, starting from the international discussion on the right to privacy and reaching the role of the Federal Revenue after the enactment of the Law, with analysis of recent specific cases and bibliographic, laws and jurisprudence research. The work goes through the discussion around the protection of personal data, analyzes the main provisions of the new Law and studies the legislation and jurisprudence that guide the treatment of information protected by fiscal and banking secrecy, placing the new Norm in the discussion. Its conception adds to the existing norms and jurisprudence and establishes the wide protection of personal data, strengthening the use that the Federal Tax Administration makes of confidential information in the fulfillment of its legal competence.

Keywords: Right to privacy; General data protection law; Federal Revenue Service; Fiscal and banking secrecy; Governance of data by the government.

LISTA DE SIGLAS

ADI	Ação Direta de Inconstitucionalidade
ANPD	Autoridade Nacional de Proteção de Dados
CDC	Código de Defesa do Consumidor
CTN	Código Tributário Nacional
eSocial	Escrituração Digital das Obrigações Fiscais, Previdenciárias e Trabalhistas
GDPR	General Data Protection Regulation (Regulamento Geral de Proteção de Dados)
IR	Imposto de Renda
LAI	Lei de Acesso à Informação
LC	Lei Complementar
LGPD	Lei Geral de Proteção de Dados
MCI	Marco Civil da Internet
SAFARI	Système Automatisé pour les Fichiers Administratifs et le Répertoire des Individus (Sistema automatizado para arquivos administrativos e diretório individual)
STF	Supremo Tribunal Federal
STJ	Superior Tribunal de Justiça

SUMÁRIO

1 INTRODUÇÃO

A Lei Geral de Proteção de Dados (LGPD) é fundamental instrumento de proteção e regulação do uso de dados pessoais em um momento em que a economia se apoia cada vez mais na coleta e manipulação desses dados, contexto em que está incluída a Receita Federal do Brasil. A edição da Lei conduziu o direito brasileiro à importante discussão sobre o tratamento sistemático de dados pessoais pelas mais diversas pessoais (físicas ou jurídicas) e entidades (públicas ou privadas), estabelecendo as bases da disciplina. Não se trata de norma editada para tratar situação específica, como o foram a Lei do *Habeas Data*, o Marco Civil da Internet e a Lei de Acesso à Informação, entre outros, mas de dispositivo de aplicação ampla e que busca disciplinar o uso de dados pessoais, protegendo-os, mas sem impedir seu uso, uma vez que é um ativo de grande valor para as empresas (crucial para sua existência, ousa-se afirmar).

No trabalho diário de uma administração tributária lida-se constantemente com dados e informações sigilosas dos contribuintes, sejam pessoas físicas ou jurídicas. Necessária a permanente análise do que é permitido ao agente público atuante na administração tributária quando da manipulação de dados sigilosos dos contribuintes, de forma que possa cumprir com seus deveres e atender à função do Ente Público sem se colocar em risco e sem prejudicar o contribuinte.

Trata-se de tema sensível e atual, uma vez que, com as novas tecnologias e avanços na computação, são coletadas muitas informações sobre os cidadãos e empresas, cuja análise faz parte da essência do trabalho de um Fisco. Ademais, como servidor público com exercício na Receita Federal, e com o consequente acesso constante a informações protegidas, faz-se necessário o conhecimento do arcabouço jurídico que trata do tema bem como dos riscos envolvidos. A edição da LGPD trouxe à tona no direito brasileiro a importante discussão sobre o armazenamento e uso de informações pessoais dos cidadãos. Nesse contexto, é fundamental analisar a atuação da Receita Federal, avaliando o impacto em seu trabalho, bem como do seu trabalho sobre essas informações.

O objetivo do presente trabalho é analisar a aplicação da Lei Geral de Proteção de Dados ao trabalho da Receita Federal. Pretende-se obter a situação atual, após a entrada em vigor da LGPD, da sua atuação e de seus agentes sobre dados protegidos/sigilosos. Mais especificamente, analisa-se o histórico das discussões sobre a proteção de dados pessoais, partindo da questão do tratamento de dados pessoais na Europa (analisa-se a GDPR e as normas que a antecederam) e as experiências brasileiras anteriores à LGPD. Em seguida, é feito estudo

dos dispositivos da LGPD relacionados ao poder público. Conclui-se o trabalho situando a LGPD dentro dos normativos que já regulam a manipulação de dados pessoais por parte do Fisco Federal, indicando as situações em que seus dispositivos interferem na coleta, armazenamento e tratamento desses dados.

Para a devida compreensão da realidade atual das discussões, o estudo inicia na análise da evolução histórica do direito da privacidade, que recentemente assumiu contornos mais voltados à tutela dos dados pessoais. Essa evolução ocorre em paralelo à evolução social, econômica e tecnológica da sociedade. Assim, uma completa análise da disciplina da tutela dos dados pessoais passa pela análise da evolução dos valores associados à informação pessoal, hoje fortemente voltados para o interesse de cada pessoa como membro ativo da sociedade.

Em seguida são analisados os dispositivos da LGPD que possuem repercussão sobre o trabalho da administração pública. A Lei é a primeira no ordenamento jurídico brasileiro com o propósito de estabelecer as bases da discussão sobre o tratamento de dados pessoais, de tal forma que sua análise necessita ser incluída na discussão sobre acesso e manipulação de dados protegidos por alguma espécie de sigilo.

As discussões relacionadas ao sigilo fiscal giravam, até o advento da LGPD, em torno do art. 198 do Código Tributário Nacional, que trata apenas da divulgação de informações econômicas ou financeiras obtidas das pessoas físicas ou jurídicas. Faz-se necessário, então, analisar se a nova normativa de proteção de dados interfere ou altera o que estava estabelecido acerca da manipulação dessas informações. A devida contextualização passa pelo estudo das discussões doutrinárias e jurisprudenciais em torno dos sigilos fiscal e bancário, institutos extensamente analisados pela justiça e pela doutrina, e estabelecidos na prática diária das administrações fiscais.

A metodologia adotada é a pesquisa exploratória, com investigação do alcance do assunto. O método de abordagem será o dedutivo, partindo do caso geral — discussão internacional sobre o direito à privacidade — para o específico — atuação da Receita Federal após a edição da LGPD. Adota-se métodos de procedimento histórico, com análise de acontecimentos ou experiências de outros países e anteriores no Brasil, e monográfico, com análise de casos específicos recentes, através de pesquisa bibliográfica, de leis e jurisprudências.

Para alcançar essa análise, este trabalho encontra-se estruturado em três capítulos. No primeiro, orientado pelo excelente trabalho de Danilo Cesar Maganhoto Doneda em Da Privacidade à Proteção de Dados Pessoais: Elementos da Formação da Lei Geral de Proteção de Dados, traz-se um estudo histórico da discussão do direito à privacidade, partindo do início

da discussão moderna, passando pelos diferentes estágios da evolução legal da disciplina até a situação atual na Europa — que inspirou fortemente a redação da Lei brasileira. Analisa-se também as iniciativas legais brasileiras relacionadas aos dados pessoais, anteriores à edição da LGPD.

O segundo capítulo se concentra na análise dos principais dispositivos da LGPD que podem repercutir no trabalho da administração pública, através do estudo da obra Lei Geral de Proteção de Dados Comentada, de Márcio Cots e Ricardo Oliveira. Assim, analisa-se as suas disposições preliminares, o capítulo específico sobre o tratamento de dados pelo poder público e as possíveis sanções administrativas aplicáveis.

Por fim, é analisada a atual situação legal da análise de dados sigilosos pela Receita Federal e onde a LGPD se encaixa nessa discussão. Busca-se contextualizar o trabalho com dados fiscais e bancários, a jurisprudência que o orienta e o que muda — se muda — com a edição da Lei. O trabalho é encerrado com um estudo dos dispositivos que tratam das boas práticas de governança dos dados e o que existe de orientação para entidades da administração pública federal sobre esse assunto.

2 O DIREITO À PRIVACIDADE E À PROTEÇÃO DE DADOS

A privacidade é uma noção cultural construída no curso do tempo por condicionantes sociais, políticos e econômicos. A origem da atual discussão jurídica da privacidade remonta ao século XIX (DONEDA, 2020, posição 1603), quando em 1846, Karl David August Röeder vislumbrou a existência de um "direito natural à vida privada", estabelecendo discussões sobre o cabimento de sua tutela.

Os fenômenos relacionados à privacidade não eram, entretanto, uma novidade para o Direito:

> Alguns estudiosos já encontraram presentes em sociedades antigas, na Grécia e China antigas, assim como em tribos hebraicas ou em sociedades iliteratas. O assunto parece ter de alguma forma ocupado os sistemas jurídicos da China antiga ou da Grécia clássica; aparece em uma manifestação mais "recente" e de evidência mais concreta, que é o *Justices of the Peace Act*, de 1361, marco do início da proteção da *privacy* no Reino Unido e que procura banir algumas práticas de intromissão em assuntos alheios (*Peeping Toms* e *eavesdropping*). (DONEDA 2020, posição 1623)

A ideia de privacidade na sua concepção moderna surge e se consolida nesse momento no âmbito da classe burguesa, como consequência do seu fortalecimento e da popularização de seus valores, em especial do individualismo. Esse processo se iniciou no fim da idade média, entre os senhores feudais mais bem colocados na sociedade, com manifestações que podem ser entendidas como indícios do surgimento de uma esfera privada em moldes que se aproximam aos atuais, como o desenvolvimento do sentimento de intimidade, ao subtrair-se pela própria vontade da vida e das ocupações em comum com outras pessoas próximas. "Intimidade durante o sono; intimidade durante as refeições, intimidade nos rituais religiosos e sociais; finalmente, intimidade no pensamento" (DONEDA, 2020, posição 1701).

Contribuiu para a evolução da ideia de privacidade o início de uma mudança nos costumes no que concerne à vida cotidiana, a partir do século XVI. A nova disposição arquitetônica das casas e cidades, que se tornam mais propícias à separação por classes e categorias e mesmo o isolamento tornaram-se regra. Duas são as causas principais apontadas pela doutrina:

> A emergência do estado-nação, da sociedade civil e das teorias de sua soberania nos séculos XVI e XVII, que formaram a noção moderna do ente público; e também o estabelecimento de uma esfera privada livre das ingerências desse ente público, como reação ao absolutismo, tendências aceleradas pelo fim da sociedade feudal e, posteriormente, pela Revolução Industrial (DONEDA, 2020, posição 1712).

Como a privacidade passa a ser prerrogativa de uma sociedade com forte componente individualista, o desenvolvimento da vida social passa a se estruturar em torno do binômio liberdade-propriedade, na qual a liberdade humana tem seu fundamento na propriedade privada, o que dá origem a uma concepção de privacidade associada diretamente à proteção da propriedade. Esta "era concebida como essencial ao desenvolvimento da própria pessoa, à realização da personalidade do indivíduo, e que, consequentemente, o direito de propriedade era a condição inafastável para chegar à privacidade" (DONEDA, 2020, posição 1731).

Segundo Doneda (2020, posição 1764), o desenvolvimento de uma noção de privacidade foi estimulado pelo surgimento da própria possibilidade material de assegurá-la. Os meios materiais à disposição, em um primeiro momento da burguesia, e que foram posteriormente massificados, providenciavam de diversas maneiras a delimitação de espaços entre os ocupantes de uma mesma casa. Tais meios era de regra fornecidos pela tecnologia, como a construção de habitações coletivas, a difusão da eletrificação e de toda a infraestrutura doméstica (hidráulica, aquecimento etc.), acompanhados de uma diminuição do número de membros para uma família média – o que implica que menos pessoas teriam necessidade de dividir seu quarto com outras.

O artigo *The right to privacy*, de Warren e Brandeis, publicado em 1890, é considerado o precursor da moderna doutrina do direito à privacidade (ZANINI, 2015). O artigo é parte de um contexto amplo no qual a sociedade norte-americana e o sistema capitalista se encontravam, e se destaca por registrar a tendência a uma fundamentação da proteção da privacidade desvinculada do direito de propriedade. Um de seus pontos centrais é a observação de que o princípio a ser observado na proteção da privacidade (no caso específico, na publicação de escritos pessoais) não passa pela propriedade privada, porém pela chamada *inviolate personality*, um direito de natureza pessoal em torno do qual a proteção da privacidade orbitará no século seguinte. Nas palavras de Warren e Brandeis,

> The principle which protects personal writings and other personal productions, not against theft and physical appropriation, but against publication in any form, is in reality not the principle of private property, but that of an inviolate personality (WARREN e BRANDEIS, 1890, p. 205).

Zanini (2015) chama atenção para as características do artigo que o tornaram tão influentes na discussão moderna sobre a privacidade: ele partia de um novo fato social, as mudanças trazidas para a sociedade pela tecnologias de informação (jornais, fotografias) e a

comunicação de massa, fenômenos que se fazem presentes na sociedade atual; e o novo "direito à privacidade", de natureza pessoal, que não mais se aproveitava da estrutura da tutela da propriedade para proteger aspectos da privacidade.

Nas décadas seguintes à publicação do artigo, a trajetória percorrida pela privacidade reflete uma mudança de perspectiva da tutela da pessoa. Após a Segunda Guerra Mundial, passou a ser citada em várias declarações internacionais de direitos. Sua primeira menção foi na Declaração Americana de Direitos e Deveres (1948), depois na Declaração Universal dos Direitos do Homem (1948), seguida da Convenção Europeia dos Direitos do Homem (1950), da Convenção Americana dos Direitos do Homem (1969), conhecida também como "Carta de San José", e mais recentemente na Carta dos Direitos Fundamentais da União Europeia (2000). Passou-se a valorizar uma esfera privada, dentro da qual a pessoa tenha condições de desenvolver a própria personalidade, livre de ingerências externas, sendo considerado pressuposto para que a pessoa não seja submetida a formas de controle social que, em última análise, anulariam sua individualidade, cercearam sua autonomia privada e inviabilizariam o livre desenvolvimento de sua personalidade.

Nas décadas seguintes a disciplina da privacidade evoluiu, ampliando a ideia inicial relacionada ao direito de se isolar, com um raciocínio em termos de espaços e bens, para um contexto de "administração" das escolhas pessoais como forma de projeção de sua personalidade no exterior e determinação da própria esfera pessoal. Segundo Doneda (2020, posição 1903 a 1919), a privacidade assumiu um caráter relacional, "que deve determinar o nível de relação da própria personalidade com as outras pessoas e com o mundo exterior – pela qual a pessoa determina sua inserção e exposição"; esse processo resulta no fortalecimento de uma esfera privada do indivíduo, necessário para a construção da individualidade e o livre desenvolvimento da personalidade sem a pressão de mecanismos de controle social.

A discussão da privacidade passou a se estruturar em torno da informação, especificamente, dos dados pessoas a partir da década de 60 (DONEDA, 2020, posição 4040), quando se desenvolveram construções legislativas e jurisprudenciais pela concepção de uma *informational privacy* nos Estados Unidos, e pelo desenvolvimento da teoria da autodeterminação informativa estabelecida pelo Tribunal Constitucional alemão e pela Diretiva 95/46/CE da União Europeia, que serão analisados à frente. Manteve-se um nexo de continuidade com a disciplina da privacidade, da qual, segundo o autor, a proteção dos dados pessoais é uma espécie de herdeira, atualizando-a e impondo características.

Com a proteção de dados pessoais, a privacidade passa a ser vista de forma mais abrangente, com a necessidade de considerar outros interesses, abrangendo as diversas formas

de controle tornadas possíveis com o tratamento de dados pessoais. Esses interesses vão desde o conhecimento da conduta pública e privada do cidadão, podendo chegar à devassa de atos pessoais, sem que muitas vezes sequer saiba dessa atividade ou disponha de meios para conhecer o resultado, retificá-lo ou cancelá-lo. Ainda que estas informações possam ser usadas para fins lícitos, também podem servir como instrumento de perseguição política ou opressão econômica.

A disciplina de proteção dos dados pessoais teve como um de seus fundamentos a reação contra projetos da administração pública que, na década de 1960, com a ajuda da informática, visavam obter e armazenar informações pessoais dos cidadãos, como o projeto do *National Data Center* nos EUA e o SAFARI na França.

O caso *National Data Center* teve origem por volta de 1965 (MENDES, 2008, p. 29), quando o Escritório do Orçamento (*Bureau of Budget*) norte-americano propôs a construção de uma central única de armazenamento de informações pessoais (o *National Data Center*), reunindo informações sobre os cidadãos norte-americanos disponíveis em vários órgãos da administração federal em um único banco de dados, com informações dos cadastros do Censo, dos registros trabalhistas, do fisco e da previdência social. Motivaram o projeto a possibilidade de solucionar dificuldades e contornar a perda de eficiência causadas pela fragmentação dos vários bancos de dados geridos pelo governo da época, otimizando seu acesso e uso, evitando a duplicidade de informações e racionalizando as ações do governo e a realização de planos de ação que permitissem antecipar o desenvolvimento socioeconômico ou a própria melhoria dos serviços públicos para o cidadão.

Tal projeto gerou reações de vários setores e provocou intensa discussão. O ponto do projeto que mais chamou atenção nos debates da época era o conjunto de problemas causados pela concentração em um único local de uma quantidade substancial dos dados pessoais de cada cidadão, em especial o receio generalizado de que a concentração de dados nas mãos da administração pública implicasse no excessivo crescimento do poder do governo, em afronta à tradição liberal da democracia norte-americana. As discussões do projeto foram conduzidas pelo Congresso norte-americano em uma série de audiências públicas, tendo resultado na proibição do estabelecido de um banco de dados nacional sem que a proteção da privacidade fosse observada e garantida ao máximo nível possível. Pontos relevantes do debate fizeram menção à dignidade e à proteção da personalidade como fundamento da negativa à instituição do *National Data Center* e a conclusão de que nem todas as informações sobre uma mesma pessoa possuem idêntica importância e, sendo assim, não devem ser protegidas da curiosidade alheia da mesma forma (MENDES, 2008, p. 29-30).

Outro caso emblemático que gerou discussões em torno do armazenamento e uso de dados pessoais ocorreu na França, no início da década de 1970 (DONEDA, 2020, posição 3885). O Instituto Nacional de Estatística da França, com a intenção de facilitar a comunicação e armazenamento de dados sobre os cidadãos em órgãos da administração pública, idealizou o chamado SAFARI – *Système Automatisé pour les Fichiers Administratifs et le Répertoire des Individus* (Sistema automatizado para arquivos administrativos e diretório individual, em tradução livre), que consistiria na transferência dos dados pessoais dos cidadãos franceses nas mãos da administração pública para sistemas informatizados. Em tal sistema, cada pessoa passaria a ser identificada por um número único por pessoa e invariável por toda a vida, o *Sécurité Sociale*, atribuído no momento do nascimento.

O projeto teve uma repercussão ruim o que levou o primeiro-ministro, diante da comoção, a interditar, por uma medida administrativa, qualquer interconexão de dados entre ministérios diferentes, o que teve o efeito prático de encerrar o projeto SAFARI (DONEDA, 2020, posição 3885). Como consequência das discussões, o tema da proteção de dados passou a ser visto com maior atenção pela população e acabou resultando na lei francesa de proteção de dados de 1978, conhecida como *Loi Informatique et Libertés*, em vigência até os dias de hoje (FRANÇA, 1978).

As primeiras doutrinas surgidas das discussões em torno desses projetos estatais eram baseadas na chamada autodeterminação informativa, expressão que designa o direito dos indivíduos de "decidirem por si próprios, quando e dentro de quais limites seus dados pessoais podem ser utilizados (PANEBIANCO, 2000 apud DONEDA, 2020, posição 3955). Esse conceito, com origem na doutrina norte-americana, orienta até hoje a proteção de dados pessoais na Alemanha e exerce grande influência em países do sistema jurídico-germânico, sendo inclusive um dos fundamentos da disciplina de proteção de dados de acordo com a Lei Geral de Proteção da Dados, motivo pelo qual merece ser analisado a fundo.

A expressão autodeterminação informativa ganhou destaque após ser utilizada em importante e influente decisão da Corte Constitucional Alemã em análise de lei que organizava um censo, aprovada em 1982, pela então República Federal da Alemanha. Tal lei determinava que cada cidadão deveria responder a 160 perguntas que seriam posteriormente submetidas a tratamento informatizado. Alguns pontos geraram controvérsias, como o que possibilitava que os dados obtidos fossem confrontados com os dados do registro civil; um outro que possibilitava que estes mesmos dados, desde que não identificados com o nome de cada titular, pudesse ser transmitido às autoridades federais e a existência de uma multa pecuniária, relativamente alta, para os que não respondessem ao questionário (MENDES, 2008, p. 46). Esses e outros pontos

geraram o temor de que, além do propósito, original, estatístico, as informações poderiam ser utilizadas para realizar controle mais rígido dos cidadãos alemãs, o que acabou por provocar o processo decidido pelo Tribunal.

A influência da decisão alemã se faz perceber no entendimento de que a proteção de dados pessoais requer um embasamento constitucional direto, como um direito fundamental, o que permite a tutela da personalidade mesmo em uma área específica como a proteção de dados.

2.1 GERAÇÕES DA TUTELA DE DADOS PESSOAIS

A disciplina de proteção de dados passou por evolução desde as primeiras experiências na década de 60, levando a doutrina a dividir as iniciativas legais em quatro gerações. A passagem de gerações refletiu a evolução e amadurecimento da sua discussão, mas também os contextos sociais e tecnológicos de cada período.

A primeira geração, em meados da década de 60, parte da reação a projetos públicos, como o caso *National Data Center* e similares, e foi marcada pela convicção de que direitos e liberdades fundamentais estariam ameaçadas pela coleta ilimitada de dados pessoais, então realizada basicamente pelo Estado.

Segundo o Doneda (2020, posição 4075), os princípios de proteção presentes nessas primeiras leis eram abstratos e amplos, focalizados basicamente na atividade de processamento de dados, além de regras específicas dirigidas aos agentes diretamente responsáveis pelo processamento dos dados. Elas eram condicionadas pela informática, pois tratavam de "bancos de dados" e não da "privacidade", não previam a participação dos cidadãos no processo de autorização e previam a existência de um comissário para proteção dos dados pessoais. O aumento na quantidade de centros de processamento de dados dificultou a eficácia dessas primeiras leis, pela complexidade em manter um controle baseado em um regime de autorizações, rígido e detalhado, que demandavam minucioso acompanhamento. São exemplos dessas primeiras leis a Lei do Land alemão de Hesse, em 1970; a primeira lei nacional de proteção de dados da Suécia, o Estatuto para bancos de dados de 1973 – *Data Legen* 289 ou *Datalag*; além do *Privacy Act* norte-americano de 1974.

A segunda geração é identificada em normas produzidas a partir da segunda metade da década de 70. Surgiram como resposta à insatisfação dos cidadãos pelo uso por terceiros de seus dados pessoais e pela carência de instrumentos para defender seus interesses, além da inviabilidade dos controles minuciosos idealizados pelas leis anteriores, que foram incapazes de acompanhar a explosão no número de centros de processamento de dados.

A principal característica das leis dessa geração é que sua estrutura passa a ser baseada na consideração da privacidade e na proteção dos dados pessoais como uma liberdade negativa, a ser exercitada pelo próprio cidadão. Foi criado um sistema que fornece instrumentos para o cidadão identificar o uso indevido de suas informações pessoais e propor a sua tutela. Em substituição da anterior, nova técnica de controle se baseava na simples notificação da criação do centro de processamento de dados. A atividade de supervisão das autoridades de controle transforma-se em uma atuação como *ombudsman* (alguém encarregado de receber e investigar queixas e reclamações), como auxiliar da administração pública ou mesmo como órgão para-jurisdicional.

Também houve problemas com essas leis. O grande poder de tutela de seus dados pessoais, com possibilidade de questionar ou interromper o seu fluxo podia implicar em o cidadão prejudicar a própria efetivação social, que já se era apoiada no fornecimento de dados pessoais. Tanto o Estado como os entes privados utilizavam intensamente o fluxo de informações pessoais para seu funcionamento. Conforme Doneda (2020, posição 4111), são exemplos dessa segunda geração a lei francesa de proteção de dados pessoais de 1978, intitulada *Informatique et Libertés* (FRANÇA, 1978), a Lei Austríaca nº 565, de 1978, além das constituições portuguesa e espanhola.

As leis de terceira geração surgem na década de 80, procurando aperfeiçoar a tutela dos dados pessoais, que continuou centrada no cidadão, mas passou a abranger mais do que a liberdade de fornecer ou não seus dados pessoais, preocupando-se também em garantir a efetividade desta liberdade. Estas leis passam tratar a proteção de dados como um processo mais complexo, estabelecendo meios de proteção para as ocasiões em que sua liberdade de decidir livremente é cerceada por eventuais condicionantes – buscando o efetivo exercício da autodeterminação informativa. O desenvolvimento destas leis tem como marco a decisão da Corte Constitucional Alemã no caso da lei do censo. Estas leis foram influenciadas também pela proliferação dos bancos de dados interligados em rede e a crescente dificuldade em localizar fisicamente o armazenamento e a transmissão de dados pessoais. São exemplos desse período as emendas às leis de proteção de dados na Alemanha e na Áustria, além de leis específicas na Noruega e Finlândia.

O tratamento de dados pessoais era visto, nesse momento, como um processo que ia além da simples permissão ou não da pessoa à utilização de seus dados pessoais, pois procurava fazer com que a pessoa participasse consciente e ativamente nas fases sucessivas do processo de tratamento e utilização de sua própria informação por terceiros. Leciona Doneda (2020, posição 4162) que “as leis dessa época encaravam a participação do cidadão como mola

propulsora de sua estrutura". Entretanto, continua o jurista, percebeu-se que, dados os custos sociais e econômicos envolvidos, não seriam muitas as pessoas dispostas a exercitar suas prerrogativas de autodeterminação informativa, dados que esses custos as compeliam a aquiescer com situações que não eram as ideais.

As leis de quarta geração, em vigência em vários países, buscam suprir as desvantagens do enfoque individual existente até então. Nestas é feito um tratamento do problema integral da informação, não mais baseando a tutela dos dados pessoais simplesmente na escolha individual, mas em instrumentos que ampliem o padrão coletivo de proteção. As leis buscam fortalecer a posição da pessoa em relação às entidades que coletam e processam seus dados, reconhecendo o desequilíbrio nessa relação. Uma característica importante é a redução do papel da autodeterminação informativa, pois se parte do pressuposto de que determinadas modalidades de tratamento de dados pessoais necessitam de uma proteção no seu mais alto grau, à qual não pode ser conferida exclusivamente a uma decisão individual, materializado em legislações que vedam absolutamente o tratamento de dados sensíveis, de forma que nem mesmo a autorização da pessoa a qual se referem os dados possa torná-la lícita. Doneda (2020, posição 4162) acrescenta como características dessa geração a disseminação de modelos de autoridades nacionais independentes para acompanhar a aplicação da lei e o surgimento de normas mais específicas, direcionadas a alguns setores de processamento de dados (como os setores de saúde e de crédito ao consumo).

2.2 PRINCÍPIOS DA PROTEÇÃO DE DADOS PESSOAIS

A doutrina identifica alguns princípios básicos, presentes nos diversos ordenamentos, em torno dos quais se desenvolveu a matéria da proteção de dados pessoais (DONEDA, 2020, posição 4215). Alguns destes princípios encontram-se presentes nas leis de primeira e segunda geração, tendo sido desenvolvidos pelas leis posteriores. Com o desenvolvimento da disciplina, a doutrina identifica cinco princípios básicos.

O princípio da publicidade (ou da transparência), pelo qual a existência de um banco de dados com dados pessoais deve ser de conhecimento público, seja mediante a exigência de autorização prévia para funcionar, da notificação a uma autoridade sobre sua existência, ou na divulgação de relatórios periódicos.

O princípio da exatidão (ou qualidade dos dados), pelo qual os dados armazenados devem ser fiéis à realidade, o que compreende a necessidade de que sua coleta e seu tratamento

sejam feitos com cuidado e correção, e de que sejam realizadas atualizações periódicas conforme a necessidade.

O princípio da finalidade, pelo qual toda utilização dos dados pessoais deve obedecer à finalidade conhecida pelo interessado antes da coleta de seus dados. Este princípio possui grande relevância prática: com base nele, fundamenta-se a restrição da transferência de dados pessoais a terceiros, além do que pode, a partir dele, estruturar-se um critério para valorar a razoabilidade da utilização de determinados dados para uma certa finalidade (fora da qual haveria abusividade).

O princípio do livre acesso, pelo qual o indivíduo tem acesso ao banco de dados onde suas informações estão armazenadas, podendo obter cópias destes registros, com a consequente possibilidade de controle destes dados; depois deste acesso e de acordo com o princípio da exatidão, as informações incorretas poderão ser corrigidas e aquelas obsoletas ou impertinentes poderão ser suprimidas, ou mesmo poder-se-á proceder a eventuais acréscimos.

O princípio da segurança física ou lógica, pelo qual os dados devem ser protegidos contra os riscos de seu extravio, destruição, modificação, transmissão ou acesso não autorizado.

A esses princípios, a Lei Geral de Proteção de Dados (BRASIL, 2018) acrescenta outros cinco em seu art. 6º, além de determinar que o tratamento de dados pessoais deverá observar a boa-fé. São eles o princípio da adequação (inciso II), que visa garantir compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento; o princípio da necessidade (inciso III), que limita o 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; o princípio da prevenção (inciso VIII), que determina a adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais; o princípio da não discriminação (inciso IX), para impossibilitar a realização do tratamento para fins discriminatórios ilícitos ou abusivos; e o princípio da responsabilização e prestação de contas (inciso X), que exige a demonstração, pelos responsáveis pelo tratamento dos dados, 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.

2.3 EXPERIÊNCIA EUROPEIA

Importantes discussões acerca da proteção de dados pessoais se desenvolveram na Europa, trazendo a disciplina ao amadurecimento de hoje, em que a tutela dos dados pessoais é

relacionada aos direitos humanos e às liberdades fundamentais, como um pressuposto do estado democrático.

Um marco da discussão da proteção de dados pessoais, que estabeleceu a estrutura que viria a dominar as discussões e legislações do continente europeu, se deu no âmbito do Conselho da Europa. Em 1981, o Conselho decidiu tratar da matéria de proteção de dados com uma convenção, realizando a Convenção para a Proteção de Indivíduos com Respeito ao Processamento Automatizado de Dados Pessoais, também conhecida como Convenção de Strasbourg ou simplesmente Convenção 108. O propósito era incitar os estados-membros do Conselho da Europa e demais signatários da Convenção a adotar normas específicas para o tratamento de dados pessoais. A Convenção 108 é consequência do entendimento do Conselho da Europa da proteção de dados como um tema de direitos humanos, orientado pelo artigo 8º da Convenção Europeia dos Direitos do Homem (artigo que trata do Direito ao respeito pela vida privada e familiar) (ARAÚJO e OLIVEIRA, 2014, p. 286).

Ainda em seu preâmbulo (UNIÃO EUROPEIA, 1981), a Convenção deixa claro que a proteção de dados pessoais se refere diretamente à proteção dos direitos humanos e das liberdades fundamentais, entendendo-a como pressuposto do estado democrático e trazendo para esse campo e disciplina, evidenciando sua referência ao artigo 8º da Convenção Europeia para os Direitos do Homem.

Em seu passo seguinte, o modelo europeu de proteção de dados estruturou-se, então, em torno da Diretiva 95/46/CE (cuja função básica no direito europeu é de uniformização legislativa), uma disciplina ampla e detalhada a ser transposta (adaptação, por cada país membro, da Diretiva ao seu próprio ordenamento jurídico) para a legislação interna de cada estado-membro (UNIÃO EUROPEIA, 1995).

A Diretiva é o documento que efetivamente padroniza a proteção de dados pessoais. Proveniente do Parlamento Europeu e do Conselho, em seus próprios termos, trata da proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Tal passo foi necessário para garantir uma melhor harmonia entre as legislações dos estados-membros da União Europeia, uma vez que uma Diretiva impõe aos legisladores dos estados a obrigação de aprovar normas alinhadas a ela.

Chama atenção o duplo propósito da Diretiva: se ela, por um lado, procura proteger a pessoa em relação ao tratamento de seus dados pessoais, por outro se destaca sua missão de induzir o comércio através do estabelecimento de regras comuns para proteção de dados na região, conforme se extrai da sua segunda consideração:

> (2) Considerando que os sistemas de tratamento de dados estão ao serviço do Homem; que devem respeitar as liberdades e os direitos fundamentais das pessoas singulares independentemente da sua nacionalidade ou da sua residência, especialmente a vida privada, e contribuir para o progresso económico e social, o desenvolvimento do comércio e o bem-estar dos indivíduos; (UNIÃO EUROPEIA, 1995).

Na consideração (4) a Diretiva reconhece a importância do tratamento de dados pessoais nos diversos domínios das atividades econômicas e sociais:

> (4) Considerando que o recurso ao tratamento de dados pessoais nos diversos domínios das actividades económicas e sociais é cada vez mais frequente na Comunidade; que o progresso registado nas tecnologias da informação facilita consideravelmente o tratamento e a troca dos referidos dados (UNIÃO EUROPEIA, 1995).

Verificamos, portanto, a presença dos dois eixos em torno dos quais a disciplina se estrutura – a proteção da pessoa e a necessidade de proporcionar a livre circulação de pessoas, mercadorias, serviços e capitais no espaço comunitário, o que implica a circulação de dados pessoais – bem como a presença de um critério de equilíbrio entre ambos que é a referência ao homem e aos seus direitos fundamentais, reconhecida como base e fundamento de toda a disciplina.

A Diretiva 46/95/CE estabeleceu ainda uma terminologia básica em seu artigo 2º. No artigo 6º ela estabelece os princípios que devem ser seguidos pelos estados-membros de modo a garantir a defesa dos interesses protegidos, além de compreender uma série de limites e exceções ao tratamento de dados pessoais na sua coleta, tratamento e utilização, como o princípio da finalidade, da publicidade, do acesso e da segurança física e lógica. Outra grande preocupação da diretiva foi sobre o tráfego de informações entre fronteiras (consideração 5): prevê-se o fluxo livre de dados entre as fronteiras dos estados-membros; já o fluxo para outros países é regulado pelo princípio da equivalência (artigos 25 e 26), pelo qual é cerceada a transmissão para países que não possuem um nível de proteção de dados pessoais considerado adequado, de acordo com os padrões da diretiva (UNIÃO EUROPEIA, 1995).

O modelo europeu alcançou a uniformidade de hoje apenas com a entrada em vigor do Regulamento Geral de Proteção de Dados (conhecido pela sigla em inglês GDPR – General Data Protection Regulation) em maio de 2018 (após aprovação pelo Parlamento Europeu em 2016). Até então estava disciplinada na Diretiva 95/46/CE, que apesar de minuciosa, a sua aplicabilidade direta ocorria apenas em via de exceção, já que a lei efetivamente aplicada aos casos concretos era a lei nacional, resultado da transposição da diretiva por cada estado membro. Essa fragmentação inspirou a atualização da normativa europeia justamente na forma de regulamento, que possui aplicabilidade direta em todos os países membros, sem a

necessidade de um procedimento de transposição. Essa aplicabilidade direta do GDPR não substitui completamente as legislações já existentes sobre a matéria nos diversos países, uma vez que estas ainda devem tratar de aspectos de natureza operacional ou espaços deixados explicitamente pelo GDPR (DONEDA, 2020, posição 4852).

A GDPR (UNIÃO EUROPEIA, 2016) é importante evolução na proteção de dados por ser norma rígida se comparada com as suas antecessoras. Ela se aplica a qualquer empresa que processe dados pessoais de cidadãos ou residentes na União Europeia, ainda que a empresa não esteja localizada na Europa. Em caso de mal uso dos dados, essas empresas estão sujeitas as penalidades, que podem chegar a 20 milhões de euros ou 4% do faturamento da empresa, o que for maior (art. 83).

A GDPR inova também nas regras relacionadas ao consentimento para o processamento de informações (UNIÃO EUROPEIA, 2016), determinando que o consentimento do titular dos dados deverá ser dado mediante um ato positivo claro que indique uma manifestação de vontade livre, específica, informada e inequívoca (consideração 32). As requisições para consentimento devem ser apresentadas de forma que a distingue claramente de outros assuntos de modo inteligível e de fácil aceso e em uma linguagem clara e simples, possuindo o titular dos dados o direito de retirar o consentimento a qualquer momento (art. 7º).

Por fim, a GDPR enumera no capítulo III direitos dos titulares de dados: direito de ser informado pelo responsável pelo tratamento quando ocorrer o armazenamento dos dados; de acesso pelo titular junto ao responsável a confirmação se seus dados são ou não objeto de tratamento e detalhes desse tratamento (finalidade, categorias dos dados, destinatários, prazo de conservação, entre outros); de retificação de dados inexatos que lhe digam respeito; à exclusão de dados (direito de ser esquecido); de limitação do tratamento em situações específicas; de portabilidade de dados que é a transmissão dos dados de um responsável pelo tratamento para outro, em um formato estruturado, de uso corrente e de leitura automática, nas situações autorizadas pelo titular; de objeção/oposição ao tratamento de seus dados; e em relação aos perfis e tomadas de decisões automáticas de não ficar sujeito a nenhuma decisão tomada exclusivamente com base no tratamento automatizado, incluindo a definição de perfis.

Um último detalhe a ser observado é que as regras da GDPR não fazem distinção quanto a dados coletados pelo poder público ou pelo setor privado, encontrando-se ambos sob as mesmas regras.

2.4 EXPERIÊNCIAS NO BRASIL ANTERIORES À LEI GERAL DE PROTEÇÃO DE DADOS

A proteção de dados pessoais no ordenamento brasileiro somente se estruturou em torno de um conjunto normativo unitário muito recentemente com o Marco Civil da Internet (Lei 12.965/2014) e com a Lei Geral de Proteção de Dados (Lei 13.709/2018). Antes, encontramos apenas a tutela constitucional tratando do problema da informação e de pontos específicos da privacidade, e alguns dispositivos em legislações ordinárias.

A Constituição tutela a informação por meio de garantias à liberdade de expressão (art. 5º, IX e art. 220) e do direito à informação (art. 5º, XIV, XXXIII e XXXIV; e art. 220). Além disso, considera invioláveis a vida privada e a intimidade (art. 5º, X), estabelece a garantia da inviolabilidade especificamente para a interceptação de comunicações telefônicas, telegráficas ou de dados (art. 5º, XII), bem como institui a ação de *habeas data* (art. 5º, LXXII), que basicamente estabelece uma modalidade de direito de acesso e retificação dos dados pessoais. A Constituição ainda protege uma série de aspectos específicos relacionados à privacidade, proibindo a invasão de domicílio (art. 5º, XI) e a violação de correspondência (art. 5º, XII).

A legislação ordinária, por sua vez, abrange um conjunto de situações, tanto existenciais como patrimoniais (DONEDA, 2020, posição 7031), nas quais se verifica a necessidade de se levar em conta interesses relacionados à privacidade. Nesse sentido, há disposições esparsas, seja no direito civil (nas disposições que estabelecem limitações ao direito de construir, nos arts. 1.301 e 1.302), bem como outras de natureza de processual (nas situações em que o processo deva correr em segredo de justiça), penal (este realiza a tutela penal da privacidade por meio de uma série de tipos que dizem respeito à violação de domicílio, correspondência e dos segredos, nos arts. 150 a 154 do Código Penal), tributária (o art. 198 do Código Tributário Nacional prevê a obrigação de sigilo para os agentes do Fisco) e em outras normas setoriais (Estatuto da Criança e do Adolescente – 8069/90 e Lei do Sistema Financeiro Nacional – 4.595/64) nas quais algum aspecto da proteção da privacidade assume relevo. Há ainda instrumentos de natureza regulatória, tais como códigos de conduta e autorregulamentação ou normas com parâmetros a serem observados entre determinadas classes profissionais para variações do sigilo profissional, como o Código de Ética Médico.

Possuindo a privacidade tutela constitucional e não existindo a mesma tutela para a proteção de dados pessoais, existe no direito brasileiro a interpretação de que as informações pessoais em si são protegidas somente em relação à sua "comunicação", conforme art. 5º, XII,

que trata da inviolabilidade da comunicação de dados, mas que não proporciona uma tutela efetiva aos dados pessoais na amplitude que a importância do tema hoje merece.

Os principais dispositivos para proteção de dados no ordenamento brasileiro, antes da Lei de Acesso à Informação, do Marco Civil da Internet e da LGPD, eram a ação de *habeas data*, introduzida pela Constituição de 1988 e regulamentada pela Lei 9.507/97, e os preceitos sobre a proteção aos dados pessoais em relações de consumo, determinados pelo Código de Defesa do Consumidor em seus artigos 43 e 44.

O Código de Defesa do Consumidor (CDC), Lei 8.078/90, em seu artigo 43, estabelece uma série de direitos e garantias para o consumidor em relação às suas informações pessoais presentes em bancos de dados e cadastros. Assim, por exemplo, o registro de dados negativos sobre o consumidor não poderá ser mantido por período superior a 5 anos; é prevista a necessidade de comunicação escrita sobre o tratamento da informação ao consumidor em certos casos, assim como o direito de acesso, correção e, implicitamente, o cancelamento justificado.

Da análise desses artigos do CDC, é possível identificar a presença de alguns dos princípios de proteção de dados pessoais indicados no item 2.2, ainda que de forma resumida e restrita ao contexto das relações de consumo. O *caput* do artigo 43 traz previsão de acesso pelo consumidor das informações arquivadas sobre ele (princípio do livre acesso); os parágrafos 1º e 3º exigem que os dados armazenados sejam claros, verdadeiros e garante a possibilidade de o consumidor exigir sua imediata correção em caso de inexatidão (princípio da inexatidão); e o parágrafo 2º garante ao consumidor o conhecimento sobre o armazenamento de suas informações, quando não solicitada por ele.

O *habeas data*, por sua vez, é um instituto idealizado pelo legislador brasileiro, concebido para proporcionar ao cidadão um instrumento para conhecer, retificar e anotar as informações sobre sua própria pessoa armazenadas em bancos de dados públicos ou bancos de dados privados de caráter público (FERNANDES, 2017).

Dalmo de Abreu Dallari relaciona a origem do *habeas data* a uma reação ao período em que o país esteve sob o comando da Ditadura Militar, que se deu quando a sociedade e o próprio ordenamento se recompunham de um período no qual diversas liberdades individuais foram suprimidas. Pontua o autor (DALLARI, 2002, p. 93) que antes da assembleia constituinte não havia referência na doutrina brasileira de qualquer proposta de criação de uma garantia constitucional dessa espécie.

O dispositivo do *habeas data* está previsto no art. 5º, LXXII, da Constituição Federal (BRASIL, 1988):

> LXXII - conceder-se-á habeas data:
> a) para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público;
> b) para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo;

A doutrina chama atenção para o termo impetrante (DALLARI, 2002, p. 103 - 104), legitimado da ação, que pode mover a ação para conhecer apenas as informações que dizem respeito à sua pessoa. Ela originalmente teve interpretação mais restritiva, de que "morreria com seu titular", o que impediu seu uso por familiares de desaparecidos na ditadura para obter mais informações.

O *habeas data*, porém, possui importantes limitações. Oferece como proteção uma ação judicial (e isso somente após prévia tentativa administrativa) que, diferentemente do *habeas corpus*, exige um advogado para sua interposição. Ademais, além da via administrativa ser incerta, o seu não atendimento não acarreta nenhuma penalidade objetiva ao responsável pelo armazenamento dos dados (DONEDA, 2020, posição 7263).

3 A LEI GERAL DE PROTEÇÃO DE DADOS E O PODER PÚBLICO

A disciplina de análise de dados pessoais hoje se encontra consolidada na Lei 13.709, de 14 de agosto de 2018, intitulada Lei Geral de Proteção de Dados (LGPD). A Lei assumiu a função de estabelecer legalmente as bases da disciplina de tratamento de dados pessoais, trazendo didaticamente em seus artigos iniciais os fundamentos, seu alcance, importantes situações excepcionais, conceitos utilizados e os princípios que a ordenam. Disciplina ainda, em capítulo específico, o tratamento de dados pelo Poder Público, objeto de estudo do presente trabalho. Diante da importância e impacto da sua edição, é fundamental sua análise e localização dentro do ordenamento jurídico brasileiro, bem como a identificação das situações em que suas disposições podem interferir no trabalho de agentes públicos.

Cumpre ressaltar que, conforme Federighi e Chow (2020, p. RR-12.6), com a edição da LGPD o legislador não alterou o núcleo fundamental do direito à privacidade, sendo a lei uma adaptação do ordenamento à nova realidade da sociedade informacional, sob constante vigilância. A lei amplia a Constituição, alargando o conceito de privacidade, adaptando-a a uma realidade inexistente quando de sua discussão.

Em relação à administração pública, a LGPD prevê a criação de uma nova entidade, responsável pela fiscalização, a Autoridade Nacional de Proteção de Dados (ANPD), inicialmente vinculada ao Poder Executivo e posteriormente independente. Ademais, a lei expressamente autoriza e enumera situações de tratamento de dados pela administração pública, para execução de políticas públicas previstas legalmente ou respaldadas em contratos, convênios ou instrumentos congêneres.

A constituição faculta às administrações tributárias identificar, respeitados os direitos individuais e nos termos da lei, o patrimônio, os rendimentos e as atividades econômicas do contribuinte (art. 145, § 1º). Essa autorização é necessária, uma vez que o tratamento de dados pessoais pelo setor público é o caminho para a viabilização de suas políticas públicas. Para que se mantenha cumprindo esse objetivo é necessário, portanto, que a administração pública se adeque à LGPD (FEDERIGHI e CHOW, 2020, p. RR-12.7).

3.1 NORMAS ANTECEDENTES À LGPD

A LGPD não é esforço isolado para a proteção das informações dos cidadãos, mas a organização de um sistema de proteção que se fortaleceu recentemente. Antes de sua edição, a

disciplina da proteção de dados estava pulverizada em leis e decretos esparsos. Além dos dispositivos constitucionais, do *habeas data* e dos dispositivos do Código de Defesa do Consumidor analisados no capítulo anterior, fazem parte desse grupo de normas, entre outros mais específicos, a Lei de Acesso à Informação (Lei 12.527/2011), que regulamentou o princípio constitucional de acesso à informação perante o poder público (artigo 5º, XXXIII da Constituição Federal) e o Marco Civil da Internet (Lei 12.965/2014), diploma idealizado para especificar direitos e garantias dos usuários da rede, surgido diante da importância que o tráfego de dados pela internet assumiu nas últimas décadas.

A Lei de Acesso à Informação (LAI) inova no ordenamento jurídico brasileiro ao criar definições legais importantes, diferenciando informações comuns de informações pessoais no âmbito de sua aplicação. Tais conceitos são importantes para o entendimento da disciplina da proteção dos dados pessoais:

> Art. 4º Para os efeitos desta Lei, considera-se:
>
> I - informação: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;
>
> II - documento: unidade de registro de informações, qualquer que seja o suporte ou formato;
>
> III - informação sigilosa: aquela submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado;
>
> IV - informação pessoal: aquela relacionada à pessoa natural identificada ou identificável;
>
> V - tratamento da informação: conjunto de ações referentes à produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle da informação;
>
> VI - disponibilidade: qualidade da informação que pode ser conhecida e utilizada por indivíduos, equipamentos ou sistemas autorizados;
>
> VII - autenticidade: qualidade da informação que tenha sido produzida, expedida, recebida ou modificada por determinado indivíduo, equipamento ou sistema;
>
> VIII - integridade: qualidade da informação não modificada, inclusive quanto à origem, trânsito e destino;
>
> IX - primariedade: qualidade da informação coletada na fonte, com o máximo de detalhamento possível, sem modificações. (BRASIL, 2011)

A LAI regulamenta em seu art. 31 o uso de informações pessoais pelo poder público, indicando a forma como se dará, prevendo responsabilização pelo mau uso e indicando situações em que o consentimento é dispensado:

> 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.
>
> § 1º As informações pessoais, a que se refere este artigo, relativas 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.
>
> § 2º Aquele que obtiver acesso às informações de que trata este artigo será responsabilizado por seu uso indevido.
>
> § 3º O consentimento referido no inciso II do § 1º não será exigido quando as informações forem necessárias:
>
> I - à prevenção e diagnóstico médico, quando a pessoa estiver física ou legalmente incapaz, e para utilização única e exclusivamente para o tratamento médico;
>
> II - à realização de estatísticas e pesquisas científicas de evidente interesse público ou geral, previstos em lei, sendo vedada a identificação da pessoa a que as informações se referirem;
>
> III - ao cumprimento de ordem judicial;
>
> IV - à defesa de direitos humanos; ou
>
> V - à proteção do interesse público e geral preponderante.
>
> § 4º 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.
>
> § 5º Regulamento disporá sobre os procedimentos para tratamento de informação pessoal. (BRASIL, 2011)

Outro ato normativo importante para a proteção de dados pessoais, embora limitado àqueles que transitam pela Internet, é a Lei 12.965/2014, intitulada Marco Civil da Internet (MCI). O Marco, combinado com sua regulamentação, o Decreto nº 8.771/2016, aborda consideravelmente o tratamento de dados pessoais, com pretensão semelhante à LGPD, com diversos dispositivos similares, como os conceitos utilizados, princípios e fundamentos, ignorando, entretanto, os dados que não circulam pela Internet, mantendo, assim, vários dados importantes fora de seu alcance:

> Todavia, apesar das semelhanças, o MCI tem a clara limitação de não projetar sua abrangência sobre os dados que não circularam pela Internet, deixando de fora uma enorme massa de dados de cujos titulares permaneceriam desguarnecidos, justificando a criação de norma mais ampla, no sentido dos seus limites, mas também mais específica, ou seja, que tivesse no seu cerne a proteção dos dados pessoais. (COTS e OLIVEIRA, 2020, pág. 40)

Ambas as leis tratam direta ou indiretamente dos temas ligados à privacidade, intimidade e dados pessoais, mas com alguma limitação ou com determinações específicas a determinado ambiente. A LGPD supre a carência, sendo a principal legislação existente sobre o tema, incluindo o estabelecimento de fundamentos e princípios que vão além da própria lei, norteando e aclarando o pensamento jurídico (COTS e OLIVEIRA, 2020, p. 42).

3.2 DISPOSIÇÕES PRELIMINARES DA LGPD

Antes da análise do capítulo específico da LGPD que trata do processamento de dados pelo poder público (capítulo IV), faz-se necessária a análise das disposições preliminares da Lei, artigos 1º a 6º, que delimita o que trata a Lei (art. 1º), os fundamentos que segue (art. 2º), seu alcance territorial (art. 3º), exceções à sua aplicação (art. 4º), conceitos e termos utilizados em seus dispositivos (art. 5º) e os princípios que a orientam (art. 6º).

Conforme Doneda no prefácio do livro de Cots e Oliveira (2020, p. 8) "a LGPD compreende uma nova sistemática e abordagem jurídica para o problema da regulamentação do uso da informação pessoal e da garantia dos direitos do seu titular, de forma que não poderia ser realizada com o instrumental jurídico anterior". A LGPD cumpre isso, segundo o jurista, pela introdução ao ordenamento jurídico brasileiro de novos elementos e conceitos, apresentando-os de forma objetiva e didática.

3.2.1 Definição e alcance

O primeiro artigo da LGPD já aponta o alcance da Lei, indicando dispor sobre o tratamento de dados pessoais, em qualquer meio, inclusive digitais. Indica também que se aplica à proteção de pessoas físicas, "com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural" (BRASIL, 2018), em harmonia com o entendimento moderno de que a privacidade é um direito fundamental, necessário para o desenvolvimento completo e amplo do ser humano. Aponta ainda os destinatários da Lei, pessoas naturais ou pessoa jurídica de direito público ou privado, em uma abrangência total.

> Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural (BRASIL, 2018).

Merece destaque que a LGPD se aplica independente do meio, sejam dados tratados por meio da Internet (*on-line*) ou *offline*. Quanto aos dados *on-line* a LGPD se soma ao Marco Civil da Internet, como normas complementares, devendo ambas serem observadas no tratamento de dados *on-line*, como se conclui do artigo 2º, parágrafo 2º, do Decreto-Lei nº 4.657/42, conhecido como Lei de Introdução às normas do Direito Brasileiro:

> § 2º A lei nova, que estabeleça disposições gerais ou especiais a par das já existentes, não revoga nem modifica a lei anterior (BRASIL, 1942).

Assim, qualquer um que trate de dados pessoais é alcançado pela lei, exceto pelos casos pontuais descritos no artigo 4º da própria lei, examinado abaixo.

Cots e Oliveira chamam atenção para a situação de não existência legal das pessoas jurídicas de direito privado, conforme disciplina o artigo 45 do Código Civil (2020, p. 47), que se inicia com a inscrição do ato constitutivo no respectivo registro, precedida, quando necessário, de autorização ou aprovação do Poder Executivo. Assim, enquanto a pessoa jurídica não for devidamente registrada, o tratamento será realizado pelas pessoas naturais envolvidas, conforme se extrai da redação do artigo 990 do Código Civil.

Ainda acerca do artigo 1º, chama-se atenção para o trecho "proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural". Conforme Cots e Oliveira (2020, p. 50), o verbo "proteger" demonstra que o legislador enxergou o titular dos dados em posição desigual em relação aos responsáveis pelo tratamento desses dados, e buscou equilibrar a relação jurídica existente entre as partes. Isso se fez necessário pois uma pessoa natural dificilmente deixará a posição de fragilidade, diante da constante incerteza de que seus dados estão ou não sendo tratados, e como estão sendo tratados. A Lei tenta mitigar essa incerteza em seu artigo 18, indicando situações em que o titular dos dados tem direito a obter do controlador informações sobre o tratamento:

> Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:
>
> I - confirmação da existência de tratamento;
>
> II - acesso aos dados;
>
> III - correção de dados incompletos, inexatos ou desatualizados;
>
> IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;
>
> V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional,

> observados os segredos comercial e industrial; (Redação dada pela Lei nº 13.853, de 2019)
>
> VI - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei;
>
> VII - informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;
>
> VIII - informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;
>
> IX - revogação do consentimento, nos termos do § 5º do art. 8º desta Lei. (BRASIL, 2018)

Por fim, o parágrafo único afirma o alcance nacional e vinculação da Lei aos demais Entes, determinando que as normas gerais contidas na Lei são de interesse nacional e devem ser observadas pela União, Estados, Distrito Federal e Municípios.

3.2.2 Fundamentos

O artigo 2º da LGPD enumera os fundamentos da disciplina de proteção de dados:

> 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. (BRASIL, 2018)

Mota e Tena (2020, p. 9) dividem os fundamentos da LGPD em três blocos distintos:

> Bloco 1 – Direitos Pessoais do Indivíduo. Envolve os fundamentos mencionados nos incisos I, II, III e IV.
>
> Bloco 2 – Desenvolvimento Econômico. Envolve os fundamentos descritos nos incisos V e VI.
>
> Bloco 3 – Desenvolvimento Humano e Social. Cuida do fundamento descrito no item VII.

O respeito à privacidade (inciso I) que, como vimos, é reconhecido como essencial ao desenvolvimento da personalidade, recebendo o status de direito fundamental, como podemos

verificar no artigo 12, da Declaração Universal dos Direitos Humanos e no inciso X do artigo 5º da Constituição Federal.

A autodeterminação informativa (inciso II), analisada no capítulo anterior, garante ao titular dos dados os elementos informativos para que possa decidir sobre o acesso a terceiros.

A Lei indica também a liberdade de expressão, informação, comunicação e opinião (inciso III), fundamentos distintos que precisam coabitar em harmonia para uma vida mais livre de perturbações, reafirmando direitos previstos na Constituição (art. 5º, IX). A liberdade de expressão atende à demanda social de proporcionar o desenvolvimento humano pois contribui para a formação da autonomia humana, dando ao homem "a prerrogativa de ser soberano de si mesmo, de ser um ente autônomo, condição esta essencial à realização pessoal" (TAVARES, 2005 apud COTS e OLIVEIRA, 2020, p. 56). Essa liberdade de expressão, entretanto, deve respeitar o direito de terceiros, especialmente relativos ao tratamento não autorizado de dados pessoais.

O inciso IV trata da inviolabilidade da intimidade, da honra e da imagem, desdobramentos do direito à privacidade, também ligados à personalidade, objetos de igual proteção legal. Sobre a intimidade, esta compõe a privacidade, mas em um âmbito mais profundo, mais secreto, onde a pessoa se desenvolve livremente, sem uma externalização dos seus atos.

O desenvolvimento econômico e tecnológico e a inovação (inciso V) segue comandos constitucionais que estabelecem que o Estado promoverá e incentivará o desenvolvimento científico, a capacitação tecnológica (art. 218) e o mercado interno com vistas à autonomia tecnológica do país (art. 219).

A livre-iniciativa, a livre concorrência e a defesa do consumidor (inciso VI) demonstram o alinhamento da LGPD com o ordenamento jurídico e reforçam seu papel de complementação desse ordenamento, para não criar embaraços ao cumprimento das determinações constitucionais. Repete nesse inciso direitos previstos na Constituição Federal, como a livre-iniciativa (art. 1º, inciso IV) e a livre concorrência e a defesa do consumidor (art. 170, incisos IV e V). Para Mota e Tena (2020, p. 7), a presença dos incisos V e VI, juntamente com a privacidade, intimidade e desenvolvimento humano, indicam que, apesar do direito à proteção de dados ser matéria relevante, não pode ser considerada como absoluto.

Por fim, a LGPD indica no inciso VII como fundamento os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais. O dispositivo alinha-se ao objetivo descrito no *caput* do art. 1º, de proteger os direitos fundamentais de liberdade e privacidade e o livre desenvolvimento da personalidade da pessoa

natural, e à Constituição Federal que estabelece como seus fundamentos, entre outros, a cidadania e a dignidade da pessoa humana (art. 1º, incisos II e III).

3.2.3 Aplicação material

O *caput* do art. 3º da LGPD dispõe sobre a sua aplicação material, não limitando o tipo de tecnologia empregada para a realização do tratamento, se por meio digital ou analógico. Aplica-se a todas as pessoas que realizam tratamento de dados, seja natural ou jurídica de direito público ou privado. A aplicação da LGPD também independe do país da sede ou do país da localização dos dados tratados.

A primeira hipótese de aplicação da Lei (inciso I) é na realização de tratamento dentro do território nacional, não fazendo distinção se o tratamento está ocorrendo pelo controlador ou pelo operador, ou se está tratando de dados de pessoas naturais estrangeiras, cujos dados tenham sido colhidos fora do território nacional. Para Vainzof (2019, p. 55), o inciso trata também do "dever de cumprimento da Lei aos agentes estrangeiros, mesmo sem sede no Brasil e que de qualquer forma 'operem' dados pessoais no Brasil, o que inclui, por exemplo, a mera coleta, produção ou recepção de dados pessoais".

A segunda hipótese diz respeito ao tratamento de dados para oferta ou fornecimento de bens ou serviços para indivíduos localizados dentro do território nacional (inciso II). Seu critério é a localização geográfica, alcançando, por exemplo, estrangeiros que estejam no território brasileiro, ainda que em férias ou por curto período de estadia. A Lei se aplicaria também a um site estrangeiro que ofereça bens e serviços aos indivíduos em nosso território. Para Cots e Oliveira (2020, p. 66), isso se confirmaria "pela análise de elementos objetivos em conjunto, tais como, idioma, entrega no endereço informado, disposições do Termo de Uso do site, entre outros".

A terceira situação de aplicação da Lei (inciso III) ocorre quando os dados pessoais objeto do tratamento tenham sido coletados no território nacional, por alguma empresa estrangeira, por exemplo. Essa hipótese é considerada redundante pela doutrina (VAINZOF, 2019, p. 67), já que a atividade de coleta está embutida no conceito de tratamento. Assim, esta terceira previsão já está incluída na primeira. Apesar desse detalhe, as hipóteses não são cumulativas, o que foi confirmado pela inclusão do "ou" ao final do segundo inciso pela Lei 13.853/2019. Conforme o §1º, a Lei considera coletados no território nacional os dados pessoais cujo titular nele se encontre no momento da coleta.

3.2.4 Situações de não aplicação

O art. 4º, citado anteriormente, trata das situações em que a LGPD não é aplicada.

> Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais:
>
> I - realizado por pessoa natural para fins exclusivamente particulares e não econômicos;
>
> II - realizado para fins exclusivamente:
>
> a) jornalístico e artísticos; ou
>
> b) acadêmicos, aplicando-se a esta hipótese os arts. 7º e 11 desta Lei;
>
> III - realizado para fins exclusivos de:
>
> a) segurança pública;
>
> b) defesa nacional;
>
> c) segurança do Estado; ou
>
> d) atividades de investigação e repressão de infrações penais; ou
>
> IV - provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei.

O inciso I trata da situação mais simples, do tratamento por pessoa natural para fins exclusivamente particulares e não econômicos, que incluiriam, por exemplo, um álbum de fotos, a agenda telefônica, anotações ou cartas antigas. Por outro lado, a título de exemplo, não se enquadrariam nessa situação, e seriam submetidas à LGPD, o armazenamento de dados pessoais em um celular corporativo se houvesse tratamento desses dados com finalidade econômica (VAINZOF, 2019, p. 70).

O segundo inciso trata do uso de dados pessoais fins jornalísticos, artísticos (alínea a) ou acadêmicos (alínea b). Para fins jornalísticos, com a liberação da atividade por qualquer pessoa, sem exigência de diploma de curso superior, e dada a profusão de informações e meios que estes circulam, tornou-se difícil identificar a atividade jornalística propriamente dita, real alvo da exceção legal em análise. Assim, Cots e Oliveira (2020, p. 70) sugerem alguns critérios para identificar as atividades jornalísticas:

> Se a empresa tem como objeto social ou atividade preponderante o jornalismo, se a notícia possui interesse público ou relevância social, se as informações são baseadas em fatos objetivos ou possuem fundamentação teórica plausível, se há a indicação de fontes confiáveis etc.

Para os fins artísticos, pode ser utilizada a Lei 9.610/98, a Lei dos Direitos Autorais, para delimitar quais são exceção da LGPD. A referida lei indica como obras do "espírito humano" (art. 7º) as obras literárias, dramáticas, musicais, coreográficas, cinematográficas, pinturas, gravuras, esculturas, ilustrações, fotos etc.

A utilização de dados pessoais para fins acadêmicos está alinhada ao desenvolvimento econômico e tecnológico e a inovação, um dos fundamentos da LGPD. Assim, o legislador trata de uma aplicação mitigada, apesar do dispositivo constar do artigo que trata de situações em que a Lei não se aplica. Conclui-se ser uma aplicação mitigada em razão da previsão da aplicação dos art. 7º e 11, que estabelecem restrições ao tratamento de dados pessoais e de dados sensíveis, respectivamente. A norma visa permitir o uso de dados públicos pelas universidades, dada a contribuição de suas pesquisas para a inovação.

Ainda no art. 4º, o inciso III descreve atividades de interesse público que estão excluídos da aplicação da LGPD, que são: segurança pública, defesa nacional, segurança do Estado ou atividades de investigação ou repressão de infrações penais. Sendo atividades de competência exclusiva do Poder Público, sua exclusão é justificada. Entretanto, os parágrafos do art. 4º estabelecem restrições para o tratamento de dados por interesse público, prevendo a edição de legislação específica, restringindo o tratamento por pessoa jurídica de direito privado ou determinando maior vigilância da autoridade nacional:

> § 1º O tratamento de dados pessoais previsto no inciso III será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei.
>
> § 2º É vedado o tratamento dos dados a que se refere o inciso III do caput deste artigo por pessoa de direito privado, exceto em procedimentos sob tutela de pessoa jurídica de direito público, que serão objeto de informe específico à autoridade nacional e que deverão observar a limitação imposta no § 4º deste artigo.
>
> § 3º A autoridade nacional emitirá opiniões técnicas ou recomendações referentes às exceções previstas no inciso III do caput deste artigo e deverá solicitar aos responsáveis relatórios de impacto à proteção de dados pessoais.
>
> § 4º Em nenhum caso a totalidade dos dados pessoais de banco de dados de que trata o inciso III do caput deste artigo poderá ser tratada por pessoa de direito privado, salvo por aquela que possua capital integralmente constituído pelo poder público. (Redação dada pela Lei nº 13.853, de 2019) (BRASIL, 2018)

A última previsão de não aplicação da LGPD está relacionada ao tratamento de dados do exterior (inciso IV), quando uma empresa brasileira poderá tratar dados oriundos do exterior, na qualidade de operador, nunca de controlador, desde que não sejam relativos às pessoas localizadas no território nacional, e desde que o país de proveniência dos dados proporcione

grau de proteção de dados pessoais adequado ao previsto na Lei. O dispositivo visa estimular a economia brasileira, tornando o país “um território receptivo e sem entraves burocráticos, do ponto de vista da proteção de dados pessoais, para empresas estrangeiras que queiram armazenar seus dados no País” (VAINZOF, 2019, p. 87).

3.2.5 Definições dos termos utilizados na Lei

O art. 5º traz, didaticamente, diversas definições legais, necessárias para o completo entendimento da discussão sobre o tratamento de dados pessoais na LGPD:

> Art. 5º Para os fins desta Lei, considera-se:
>
> I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;
>
> II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;
>
> III - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;
>
> IV - banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;
>
> V - titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;
>
> VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
>
> VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;
>
> VIII - encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD); (Redação dada pela Lei nº 13.853, de 2019)
>
> IX - agentes de tratamento: o controlador e o operador;
>
> 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;
>
> XI - anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;
>
> XII - consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;
>
> XIII - bloqueio: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados;
>
> XIV - eliminação: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;

> XV - transferência internacional de dados: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro;
>
> 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;
>
> XVII - relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco;
>
> XVIII - órgão de pesquisa: órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico; e (Redação dada pela Lei nº 13.853, de 2019)
>
> XIX - autoridade nacional: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional. (Redação dada pela Lei nº 13.853, de 2019)

Sobre as definições do art. 5º, Cots e Oliveira (2020, p. 77) chamam atenção para algumas características. O primeiro detalhe digno de nota é o critério expansionista do conceito de dados pessoais, incluindo no conceito os dados que tornam a pessoa identificável de forma indireta. Assim, se uma empresa dispõe de diversos bancos de dados que combinados identificam uma pessoa, tais dados são considerados pessoais, ainda que isoladamente não identifiquem o indivíduo. Outro ponto que os autores chamam atenção é que o rol do inciso X é exemplificativo e as atividades são não cumulativas, ou seja, uma única atividade da lista já se inclui no conceito de tratamento, mesmo as mais simples, como o armazenamento sem qualquer outra utilização. Por último, destacam a nomenclatura utilizada para a Autoridade Nacional de Proteção de Dados (disciplinada no artigo 55-A e seguintes), que no inciso XIX é chamado apenas de autoridade nacional, mas que devem ser consideradas sinônimos na leitura da LGPD.

3.2.6 Princípios da proteção de dados na LGPD

O artigo 6º encerra o capítulo das disposições preliminares da LGPD estabelecendo que as atividades de tratamento de dados pessoais deverão observar a boa-fé e dez princípios (analisados no item 2.2).

A boa-fé é princípio geral e tem papel fundamental nas relações jurídicas, conforme os artigos 113 e 422 do Código Civil (BRASIL, 2002), que estabelecem que os negócios jurídicos

devem ser interpretados e executados seguindo o princípio da boa-fé. Tendo o tratamento de dados pessoais, na maioria das vezes, natureza contratual entre o titular dos dados e o controlador, necessária a exigência desse princípio.

3.3 TRATAMENTO DE DADOS PELO PODER PÚBLICO COM A LGPD

A Lei Geral de Proteção de Dados complementou a Lei de Acesso à Informação como uma nova etapa da relação entre o Poder Público e o cidadão (Blum e López, 2020, p. 171). Ao mesmo tempo em que afirma que a Lei não se aplica ao tratamento de dados pessoais realizados com fins exclusivos de: a) segurança pública; b) defesa nacional; c) segurança do Estado; ou d) atividades de investigação e repressão de infrações penais (art. 4º), em seus parágrafos afirma que a autoridade nacional emitirá opiniões técnicas ou recomendações sobre essas exceções e poderá solicitar relatório de impacto à proteção de dados pessoais, em uma demonstração de cautela. Tais atividades descrevem atuações do Poder Público que podem gerar riscos às liberdades civis e aos direitos fundamentais, por isso se faz necessária a autuação da Lei.

A LGPD estabelece entre as hipóteses em que o tratamento de dados pessoais poderá ser realizado, aquele feito pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei (art. 7º, inciso III).

3.3.1 Regras para o tratamento dos dados pessoais pelo poder público

O tratamento de dados pessoais pelas pessoas jurídicas de direito público está disciplinado no Capítulo IV, artigos 23 a 32, da LGPD. O rol de pessoas jurídicas alcançadas por esse regramento é indicado no parágrafo único do artigo 1º da Lei 12.527/2011 (Lei de Acesso à Informação) e inclui:

> I - os órgãos públicos integrantes da administração direta dos Poderes Executivo, Legislativo, incluindo as Cortes de Contas, e Judiciário e do Ministério Público;
>
> II - as autarquias, as fundações públicas, as empresas públicas, as sociedades de economia mista e demais entidades controladas direta ou indiretamente pela União, Estados, Distrito Federal e Municípios. (BRASIL, 2011)

O *caput* do artigo 23 determina que o tratamento deverá ser realizado para o (i) atendimento de sua finalidade pública, (ii) na persecução do interesse público e com o objetivo de (iii) executar as competências legais ou cumprir as atribuições legais do serviço público. Cots e Oliveira chamam atenção que o primeiro pressuposto depende do segundo, pois a "finalidade somente é 'pública' se o interesse for 'público', isso, logicamente, porque estamos tratando de entidades governamentais" (2020, p. 158). Para os autores, interesse público e direitos fundamentais devem caminhar em harmonia, sob o risco de ocorrerem arbitrariedades ou injustiças caso o primeiro se distancie do segundo. Continuam os autores que ao condicionar o tratamento de dados à perseguição de finalidades e interesses públicos, o legislador está impedindo o tratamento em atendimento a interesses privados ou particulares.

O terceiro pressuposto, quanto à execução das competências legais ou cumprimento das atribuições legais, restringe o alcance do tratamento às finalidades de cada ente público, às funções que lhe são cometidas por lei. Como consequência dessa regra, entendem Cots e Oliveira (2020, p. 159) que "se o tratamento de dados se der fora da competência ou atribuição legal do órgão público, será considerada ilegal".

Em razão do princípio da legalidade (artigo 37 da Constituição Federal), qualquer órgão público está sempre amparado em uma disposição legal em suas ações, o que acaba por fundamentar, em algum nível, o tratamento de dados pessoais, quando executado dentro de suas competências legais. Além dessa previsão legal presente no *caput* do artigo 23, Blum e López (2020, p. 175) destacam outros dispositivos que poderão ser utilizadas para regular o tratamento de dados pelo Poder Público. Os autores indicam que em casos pontuais outras previsões legais da LGPD são aplicáveis:

> A realização de estudos por órgãos de pesquisa, sendo estes sem fins lucrativos (artigo 7º, IV); contrato ou diligência contratual de que é parte um titular de dados pessoais (artigo 7º, V); exercício regular de direitos em processos judicial, administrativo ou arbitral (artigo 7º, VI); proteção da vida ou da incolumidade física de terceiros (artigo 7º, VII); tutela da saúde (artigo 7º, VIII); interesse legítimo do controlador ou de terceiros (artigo 7º, IX) ou mesmo proteção ao crédito (artigo 7º, X). (BLUM e LÓPEZ, 2020, p. 175)

A LGPD estabelece alguns requisitos para o tratamento de dados pelo poder público. Determina que o ente deverá informar as hipóteses em que realizar o tratamento de dados pessoais, com informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas nessas atividades, em veículos de fácil acesso, de preferência em seus *sites* (inciso I do art. 23). Essa disposição é importante proteção da

transparência nas relações democráticas do Poder Público com os cidadãos. Segundo Blum e López (2020, pág. 175):

> Se em uma sociedade de informação, como a nossa, saber é poder, a transparência sobre os dados pessoais sobre os quais se sabe implica o compartilhamento do poder detido, haja vista que comprova pela clareza a legalidade de suas ações.

Nos parágrafos do artigo 23, a LGPD se integra ao ordenamento jurídico, com referências expressas a outras importantes leis que a precedem "apontando um acréscimo de prestações positivas aos cidadãos" (BLUM e LÓPEZ, 2020, p. 176). No §2º, a Lei afirma que as figuras de autoridades responsáveis pelo cumprimento das obrigações da Lei de Acesso à Informação, já instituídas pelos órgãos públicos, não se confunde com a necessidade de indicação de um encarregado pelo tratamento de dados pessoais da Lei Geral de Proteção de Dados. Por sua vez, o §3º indica a evolução democrática nos institutos de acesso e proteção dos dados, ao afirmar que os prazos e procedimentos para o exercício desses direitos perante o Poder Público observarão a legislação específica, em especial à Lei do Habeas Data (lei nº 9.507/1997), a Lei Geral do Processo Administrativo (lei nº 9.784/1999) e a Lei de Acesso à Informação (lei nº 12.527/2011).

No inciso II do artigo 23, a lei determina a indicação de um encarregado, que conforme o inciso VIII do art. 5º, é a pessoa responsável por atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD). Nesse ponto, a Lei é ainda mais rigorosa com o Poder Público (BLUM e LÓPEZ, 2020, p. 176), exigindo a indicação da autoridade mesmo que esteja no papel de operador, ante a regra geral de obrigatoriedade da indicação de um encarregado apenas pelos controladores de dados (art. 41).

O artigo 24 estabelece a sujeição das empresas públicas e sociedades de economia mista aos dispositivos do capítulo de acordo com a sua atuação. Quando atuarem em regime de concorrência, sujeitas ao disposto no art. 173 da Constituição Federal, terão o mesmo tratamento dispensado às pessoas jurídicas de direito privado particulares (*caput*). Por outro lado, aquelas que estiverem atuando na operacionalização de políticas públicas e no âmbito da execução delas, terão o mesmo tratamento dispensado aos órgãos e às entidades do Poder Público (parágrafo único).

A distinção de atuações frequentemente não é tão clara, com algumas empresas atuando de forma mista, ora no regime de concorrência ora em atividades de interesse público. Nesses casos, deve haver uma clara segregação do banco de dados de tais empresas, a fim de que "não

haja aproveitamento indevido de vantagens dedicadas aos órgãos públicos enquanto perseguem lucro não apenas para o Estado, mas também para acionistas particulares" (TASSO, 2019, p. 370).

3.3.2 Regras para o compartilhamento dos dados pessoais

A LGPD determina no artigo 25 que os dados deverão ser mantidos em formato interoperável e estruturado para uso compartilhado. O faz para estímulo e facilitação da execução de políticas públicas, da prestação de serviços públicos, da descentralização da atividade pública e da disseminação e acesso das informações pelo público em geral. Esta regra visa desestimular a adoção pelos Entes de tecnologias fechadas ou de difícil compatibilidade, que acabariam por inviabilizar o compartilhamento de dados entre eles e, por fim, o acesso por parte do próprio titular, que precisaria contratar ferramentas ou *softwares* específicos, um entrave à disseminação e acesso das informações pelo público em geral.

Ainda sobre o compartilhamento, o artigo 26 estabelece regras específicas para tais situações (comunicação e compartilhamento), determinando que deve atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas. Em seu §1º determina ser vedado a transferência a entidades privadas dados pessoais constantes de bases de dados a que tenha acesso, mas indica em seus incisos quatro exceções.

A primeira hipótese (inciso I) permite a transferência em casos de execução descentralizada de atividade pública que exija a transferência, exclusivamente para esse fim específico e determinado, observado o disposto na Lei de Acesso à Informação. Merece destaque a determinação que de que a transferência se dê exclusivamente para fim específico e determinado, entendendo-se (TASSO, 2019, p. 385) que não é permitido o compartilhamento de dados desnecessários para as finalidades pretendidas, o que seria contrário ao princípio da necessidade (art. 6º, inciso III).

A segunda hipótese está prevista no inciso III (o inciso II foi vetado) trata de possibilidade de certa forma óbvia, ao permitir as transferências de dados acessíveis publicamente.

A terceira (inciso IV) hipótese trata da possibilidade de transferência quando houver previsão legal ou for respaldada em contratos, convênios ou instrumentos congêneres.

Por fim, a quarta hipótese (inciso V) permite a transferência de dados para entidades privadas quando objetivar exclusivamente a prevenção de fraudes e irregularidades, ou para proteger a segurança ou a integridade do titular. Nessa hipótese, o interesse do titular só precisa

ser atendido na segunda parte do dispositivo. Na primeira parte o interesse pode ser público, para apurar a ocorrência de fraude em determinado programa social, por exemplo. Nesse caso, o ente público poderia comunicar os dados dos titulares sem receber deles o consentimento.

O artigo 28 estabelece os demais requisitos para o compartilhamento de dados pelo Poder Público. Seu *caput* determina que a comunicação ou o uso compartilhado de dados pessoais de pessoa jurídica de direito público a pessoa de direito privado será informado à autoridade nacional (ANPD) e dependerá de consentimento do titular. Acerca desse consentimento, a LGPD traz exceções: (i) nas hipóteses de dispensa de consentimento previstas na própria Lei, (ii) na execução de atividades de sua competência ou (iii) nas exceções para transferências constantes do §1º do art. 26, analisadas acima.

3.3.3 Tutela do Poder Público pela autoridade nacional

O legislador possibilitou que a autoridade nacional possa solicitar, a qualquer momento, informações específicas sobre os detalhes do tratamento de dados realizado. A autoridade poderá determinar adequações por meio de parecer técnico complementar, garantindo o cumprimento da LGPD (art. 29). A autoridade poderá ainda estabelecer normas complementares para as atividades de comunicação e de compartilhamento de dados pessoais, e apenas para essas atividades de tratamento, realizados por quaisquer tipos de controlador, incluindo o de direito público (art. 30). Para Cots e Oliveira (2020, p. 173), trata-se de dispositivo importante para garantir a adaptação da norma a novas realidades de tratamento de dados pessoais:

> Tal disposição é essencial, pois possibilita maior dinamismos para o tratamento de questões que serão levantadas durante a adaptação da sociedade à nova lei, impedindo que a sociedade tenha que aguardar em cenário de frequente insegurança jurídica até que a lei seja adaptada, complementada ou corrigida.

Ainda a descrever as atribuições e prerrogativas da autoridade nacional, o artigo 31 possibilita que esta, quando houver infração da lei, envie "informe com medidas cabíveis para fazer cessar a violação" (BRASIL, 2018). Tal dispositivo não deve ser entendido como um obstáculo para a aplicação de sanções administrativas estabelecidas no art. 52, uma vez que o "expediente parece ter por base a boa-fé das ações governamentais e o interesse dos gestores públicos em corrigir procedimentos que violem a LGPD" (COTS e OLIVEIRA, 2020, p. 174).

A autoridade nacional poderá também solicitar a agentes do Poder Público a publicação de relatórios de impacto à proteção de dados pessoais e sugerir a adoção de padrões e de boas práticas para o tratamento de dados pessoais pelo Poder Público (art. 32). Cots e Oliveira (2010, p. 176) entendem que o dispositivo torna obrigatório ao Poder Público a elaboração de relatórios de impacto à proteção de dados pessoais, ainda que não os torne público, aguardando deliberação da autoridade. Tasso (2019, p. 394) discorda por entender que essa conclusão seria contrária ao conceito da legalidade aplicável à administração, que deve agir segundo a lei, além de, fazendo remissão ao art. 38, destacar que a elaboração do relatório é facultativo, só sendo produzido quando a autoridade assim determinar ao controlador.

3.4 SANÇÕES ADMINISTRATIVAS

O artigo 52 da LGPD indica as sanções administrativas aplicadas pela autoridade nacional nas infrações cometidas às normas previstas na Lei. Essas infrações não se dedicam ao ressarcimento de danos, pois não são destinadas aos titulares dos dados ou a terceiros prejudicados, sendo então uma sanção administrativa retributiva, com caráter repressivo, cujo propósito é "imputar um mal ao infrator de acordo com o ato ilícito praticado" (MELLO, 2007, apud COTS e OLIVEIRA, 2020, p. 229).

Os órgãos públicos também estão sujeitos a algumas sanções administrativas da LGPD, conforme o §3º do artigo 52. Das sanções indicadas no *caput* do artigo não se aplicam aos órgãos do Poder Público a multa simples (inciso II) e a multa diária (inciso III). Isso porque, conforme Cots e Oliveira (2020, p. 237), a atividade dos referidos órgãos não se dedica ao lucro e uma imposição de penalidade pecuniária acabaria por onerar o orçamento público e precarizar os seus serviços.

Assim, poderão ser aplicadas, nos termos do §3º do artigo 52, as sanções:

> I - advertência, com indicação de prazo para adoção de medidas corretivas;
>
> [...]
>
> IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência;
>
> V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
>
> VI - eliminação dos dados pessoais a que se refere a infração;
>
> X - suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador; (Incluído pela Lei nº 13.853, de 2019)

> XI - suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período; (Incluído pela Lei nº 13.853, de 2019)
>
> XII - proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados. (Incluído pela Lei nº 13.853, de 2019)

Ainda no §3º, a aplicação das sanções administrativas não prejudica a incidência de outros diplomas legais, como é o caso da Lei 8.112, de 11 de dezembro de 1990 (Estatuto do Servidor Público Federal), da Lei 8.429, de 2 de junho de 1992 (Lei de Improbidade Administrativa), e a Lei de Acesso à Informação.

Por fim, a ANPD deverá ponderar a adequação de cada sanção ao caso concreto, evitando prejuízos à sociedade que podem ser mais graves do que o tratamento inadequado de dados pessoais pelo poder público, uma vez que "a medida é extremada e de forma alguma deverá comprometer serviços básicos, como saúde, educação, transporte, entre outros" (COTS E OLIVEIRA 2020, p. 238).

Analisados os principais dispositivos da Lei Geral de Proteção de Dados que podem repercutir sobre a atuação da administração pública, estudaremos as regras e jurisprudência a que está submetida a Receita Federal quando trata dados pessoais no exercício de sua obrigação legal e de que forma a edição de uma regulamentação geral do tratamento de dados interfere – caso interfira – nesse trabalho e na administração que faz dos dados.

4 SITUAÇÃO ATUAL DA PROTEÇÃO DE DADOS A QUE SE SUBMETE A RECEITA FEDERAL

A Lei Geral de Proteção de Dados estabelece e regulamenta a disciplina de proteção de dados pessoais no Brasil, aplicando-se indistintamente a empresas privadas e à administração pública, alcançando, portanto, a Receita Federal.

Para compor um retrato completo do tratamento de dados a que se encontra submetido o Fisco Federal e de que forma a entrada em vigência da LGPD interfere em seu trabalho, caso interfira, faz-se necessário analisar a legislação e jurisprudência que orientam o tratamento de dados pessoais dos contribuintes, em especial o sigilo fiscal e o sigilo bancário, institutos antigos e extensamente discutidos no ordenamento jurídico brasileiro. As discussões conduzidas em torno desses dois temas são guias para a aplicação e localização da nova lei de dados na coleção de normativos a que se encontra submetida a Receita Federal no cumprimento de sua atribuição legal.

4.1 FISCALIZAÇÃO TRIBUTÁRIA

O Poder Público tem o dever de efetuar a fiscalização tributária, observando se o contribuinte está cumprindo suas obrigações tributárias conforme a lei. Para isso, o sistema jurídico confere poderes aos agentes fiscais, com o intuito de garantir condições à realização dessa investigação. Conforme o § 1º do art. 145 da Constituição Federal, a Administração Tributária é competente para identificar o patrimônio, os rendimentos e as atividades econômicas dos contribuintes, devendo tal atividade respeitar os direitos individuais e prescrições legais.

Complementando as possibilidades de uso e compartilhamento das informações necessários ao cumprimento de suas obrigações legais, o inciso XXII do art. 37 da Constituição Federal prevê que as administrações tributárias da União, dos Estados, do Distrito Federal e dos Municípios atuarão de forma integrada, inclusive com o compartilhamento de cadastros e de informações fiscais, na forma da lei ou convênio. Trata-se de importante ferramenta para os Fiscos atuarem, prerrogativa concedida apenas a estes, no exercício de suas funções, e não a outras áreas da Administração Pública (MACHADO e JANINI, 2015, p. 20).

Dessa forma, há a previsão constitucional da instituição de obrigações acessórias que, nos termos do art. 113, § 2º, do Código Tributário Nacional (CTN), decorrem da legislação tributária e têm por objeto as prestações, positivas ou negativas, nela previstas no interesse da arrecadação ou da fiscalização dos tributos. As obrigações acessórias têm como conteúdo, por exemplo, a emissão de documentos fiscais, a elaboração de escrituração fiscal e a apresentação de declarações ao Fisco, como a declaração de Imposto de Renda (IR) (FEDERIGHI e CHOW, 2020, p. RR-12.9).

Os agentes fiscais recebem atribuições que lhes permitem investigar e analisar as obrigações acessórias. Tal competência gera o dever de o contribuinte suportar a fiscalização tributária, em decorrência do interesse público. Ocorre que esse dever está limitado pelos direitos fundamentais, cujo objetivo consiste em evitar uma fiscalização ilícita:

> O combate à sonegação fiscal é essencial à arrecadação tributária, bem como o respeito aos direitos fundamentais é indispensável à manutenção do Estado Democrático de Direito e à dignidade humana. Em suma, hão de conviver a fiscalização tributária e os direitos fundamentais do contribuinte. (MACHADO e JANINI, 2015, p. 20)

Assim, as informações necessárias ao trabalho das fiscalizações tributárias encontram-se protegidas por importantes normativos que tratam dos sigilos fiscal e bancário, e a atuação dos agentes fiscais está rigorosamente descrita no sistema jurídico, de forma a evitar abusos e arbitrariedades.

4.2 SIGILO FISCAL

Com a redação dada pela Lei Complementar 104/01, o art. 198 do CTN trata do sigilo fiscal, vendando 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. Esse dispositivo protege, portanto, a privacidade dos sujeitos passivos de obrigações tributárias, resguardando-os da revelação pública da sua situação econômica ou financeira, da natureza e do estado dos seus negócios para terceiros estranhos ao procedimento de fiscalização tributária (PAULSEN, 2020, p. 511).

O dispositivo prevê poucas e específicas exceções à regra geral do não fornecimento das informações fiscais. As duas primeiras hipóteses, indicadas no §1º do art. 198 do CTN, possibilitam o fornecimento de informação mediante requisição de autoridade judiciária no

interesse da justiça (inciso I), e a resposta às 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 (inciso II). Nessa última, exige o CTN que o intercâmbio de informações sigilosas 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 (§2º).

O §3º do art. 198 indica outras três situações de exceção ao sigilo fiscal, autorizando a divulgação de informações relativas a representações fiscais para fins penais (inciso I), de inscrições na Dívida Ativa da Fazenda Pública (inciso II) e de parcelamento ou moratória (inciso III).

Encerrando as situações de compartilhamento ou divulgação de informações fiscais, o art. 199 possibilita a assistência mútua entre as Fazendas da União, dos Estados e dos Municípios na fiscalização dos tributos respectivos, com a permuta de informações, alinhado com as disposições do inciso XXII do art. 37. Em seu parágrafo único, autoriza ainda a permuta de informações com estados estrangeiros, no interesse da arrecadação e fiscalização de tributos.

A possibilidade de permuta de informações com Estados estrangeiros é tratada pelo Decreto n. 8.842/16, que promulga o texto da Convenção sobre Assistência Mútua Administrativa em Matéria Tributária emendada pelo Protocolo de 1º de junho de 2010, firmada pelo Brasil em Cannes, em 3 de novembro de 2011. O seu art. 22, que trata especificamente do sigilo, estabelece que quaisquer informações obtidas por uma Parte "serão consideradas sigilosas e protegidas do mesmo modo que as informações obtidas com base na legislação interna e na medida necessária para garantir o nível necessário de proteção de dados de caráter pessoal" (BRASIL, 2016).

O art. 22 do Decreto também estabelece que

> as referidas informações só poderão ser comunicadas às pessoas ou autoridades (incluindo tribunais e órgãos de administração ou supervisão) encarregadas do lançamento, arrecadação, ou cobrança dos tributos dessa Parte, ou dos procedimentos de execução ou persecução, ou das decisões de recursos relativos a esses tributos, ou da supervisão das atividades precedentes. Apenas as pessoas ou autoridades referidas acima poderão utilizar essas informações e exclusivamente para os fins acima mencionados (BRASIL, 2016).

Cumpre mencionar também que a determinação de manutenção do sigilo fiscal do art. 198 do CTN é reforçada pelo art. 116 da Lei n. 8.112/91, lei que dispõe sobre o regime jurídico dos servidores públicos civis da União, aos estabelecer o dever desses de atender com presteza

ao público em geral, fornecendo as informações requeridas, ressalvadas as protegidas por sigilo, bem como de guardar sigilo sobre assunto da repartição. A violação desses deveres sujeita o servidor a processo administrativo disciplinar (PAULSEN, 2020, p. 512).

A violação de sigilo está tipificada no Código Penal, embora não esteja descrita em tipo específico de crime contra a ordem tributária. No capítulo dos crimes contra a liberdade individual, na seção dos crimes contra a inviolabilidade dos segredos, o Código indica o crime de violação do segredo profissional. Seu art. 154 prevê, como conduta criminosa, "Revelar alguém, sem justa causa, segredo, de que tem ciência em razão de função, ministério, ofício ou profissão, e cuja revelação possa produzir dano a outrem", cominando pena de "detenção, de três meses a um ano, ou multa" (BRASIL, 1940). Trata-se de crime de ação pública condicionada a representação (PAULSEN, 2020, p. 512).

Por fim, cumpre-nos analisar o sigilo fiscal como uma garantia fundamental. O sigilo fiscal não foi expressamente incluído no rol dos direitos e garantias fundamentais do contribuinte. Entretanto, conforme lecionam Machado e Janini (2020, p. 20), isso não impede de classificá-lo como um direito integrante do estatuto do contribuinte. Para os autores, o direito ao segredo dos dados fiscais decorre de um desdobramento necessário do direito fundamental à privacidade e do sigilo das comunicações, previstos no art. 5º, X e XII da Constituição.

Ademais, reforça esse entendimento julgamento do STJ no HC 160.646/SP, de relatoria do Ministro Jorge Mussi, julgado em 01/09/2011:

> O sigilo fiscal se insere no direito à privacidade protegido constitucionalmente nos incisos X e XII do art. 5º da Carta Federal, cuja quebra configura restrição a uma liberdade pública, razão pela qual, para que se mostre legítima, se exige a demonstração ao Poder Judiciário da existência de fundados e excepcionais motivos que justifiquem a sua adoção. (BRASIL, 2011)

O sigilo fiscal pode ser entendido, assim, como a proteção constitucional das informações prestadas pelos contribuintes ao Fisco, especialmente por meio das obrigações acessórias, contra a violação por terceiros ou para fins estranhos à fiscalização tributária. Dessa forma, compete ao ente da Administração preservar e proteger aquelas informações fiscais recebidas contra terceiros não autorizados a acessá-las, tendo em vista que "o sistema jurídico não autoriza o uso dos dados fiscais para uma finalidade diversa daquela relacionada à arrecadação e fiscalização tributária" (MACHADO e JANINI, 2015, p. 21).

A proteção do sigilo fiscal atinge, portanto, aquelas informações que já se encontram na posse do Fisco. O particular é obrigado a apresentar muitos dados referentes a salários, rendimentos, movimentações financeiras, compras, vendas, despesas, receitas etc. São

situações que integram sua vida privada e passam a ser de conhecimento da Administração Tributária, que tem o dever de zelar por elas.

Os direitos fundamentais, entretanto, não são absolutos. É o caso do sigilo fiscal. Em determinadas circunstâncias excepcionais é possível o acesso às informações fiscais do contribuinte por terceiros. Demonstra isso a analisada hipótese constitucional de compartilhamento de informações fiscais entre as administrações tributárias da União, dos Estados, do Distrito Federal e dos Municípios, nos termos do art. 37, inciso XXII, prerrogativa concedida exclusivamente ao Fisco, no exercício de suas funções, e não a outras áreas da Administração Pública. Ademais, admite-se que outras pessoas sem interesse na fiscalização tributária acessem as informações fiscais, permissão concedida apenas em casos excepcionalíssimos, indicados nos artigos 198 e 199 do CTN.

4.3 SIGILO BANCÁRIO

O art. 197 do CTN estabelece a obrigatoriedade de prestarem informações sobre bens, negócios ou atividades de terceiros para as autoridades administrativas para, dentre outros, as instituições financeiras, as administradoras de bens, os corretores e quaisquer outros que a lei designe em razão de seu cargo, ofício, função, ministério, atividade ou profissão. Preserva, contudo, em seu parágrafo único, as informações quanto aos fatos sobre os quais o informante esteja legalmente obrigado a observar segredo profissional, de modo que, nesses casos, o segredo prevalece sobre os deveres genéricos de informação tributária, só cedendo em face de autorizações legais ou judiciais específicas.

O sigilo das operações de instituições financeiras é regulada, com maior detalhamento, pela Lei Complementar nº 105, de 10 de janeiro de 2001, que determina a informação à administração tributária das operações financeiras efetuadas pelos usuários de seus serviços (art. 5º), com identificação dos titulares e dos montantes globais movimentados mensalmente (§ 2º). Conforme o art. 6º, as autoridades e agentes fiscais tributários somente poderão examinar os registros das instituições financeiras quando houver processo administrativo instaurado ou procedimento fiscal em curso e o exame seja considerado indispensável, sendo que a lei estabelece que, uma vez detentores das informações desejadas, deverão mantê-las em sigilo:

> Art. 6º As autoridades e os agentes fiscais tributários da União, dos Estados, do Distrito Federal e dos Municípios somente poderão examinar documentos, livros e registros de instituições financeiras, inclusive os referentes a contas de depósitos e aplicações financeiras, quando houver processo administrativo instaurado ou

> procedimento fiscal em curso e tais exames sejam considerados indispensáveis pela autoridade; administrativa competente.
>
> Parágrafo único. O resultado dos exames, as informações e os documentos a que se refere este artigo serão conservados em sigilo, observada a legislação tributária.

A transferência de informações bancárias para o Fisco não é considerada pela doutrina e pela jurisprudência uma quebra de sigilo propriamente dita, mas uma transferência, isso porque as informações sob sigilo bancário são repassadas para autoridades que têm obrigação de mantê-las sob sigilo fiscal, quando o seu exame seja indispensável. Assim, o sigilo bancário não ostenta caráter absoluto e a possibilidade de quebra depende da análise do caso concreto, considerando-se as suas circunstâncias específicas e o princípio da proporcionalidade (PAULSEN, 2020, pg. 508).

Por ter estendido o acesso aos dados bancários às administrações tributárias sem necessidade de autorização judicial, a LC 105/2001 foi diversas vezes contestada perante as Cortes Superiores. O ponto controverso recai na possibilidade de o sigilo de dados ser quebrado por procedimentos da autoridade administrativa sem autorização judicial, no caso da Receita Federal, em face da tutela constitucional sobre o sigilo, além do art. 197, parágrafo único, do Código Tributário Nacional, que desobriga o informante de prestar informações sobre fatos que deva manter em segredo por força de lei, em razão de cargo, ofício, função, ministério, atividade ou profissão.

As controvérsias sobre a constitucionalidade da permissão legal foram extensamente analisadas pelas Cortes e suas decisões foram alinhadas à concepção vigente no STF de que os direitos e garantias individuais não têm caráter absoluto e que em determinadas situações podem "ceder em face de outros direitos considerados mais relevantes, do interesse público ou social e da justiça, além de situações excepcionais, quando esses direitos e garantias sirvam de escudo para acobertar condutas criminosas" (ÁVILA e WOLOSZYN, 2017, p. 186).

Em 2016, o Supremo Tribunal Federal (STF), no RE 601.314, fixou tese com repercussão geral de que a norma estabelece requisitos objetivos e trata de um translado/transferência de dever de sigilo:

> O art. 6º da Lei Complementar 105/01 não ofende o direito ao sigilo bancário, pois realiza a igualdade em relação aos cidadãos por meio do princípio da capacidade contributiva, bem como estabelece requisitos objetivos e o translado do dever de sigilo da esfera bancária para a fiscal. (BRASIL, 2016)

Também em 2016, o STF analisou diversas Ações Diretas de Inconstitucionalidade (ADI) que tratavam da Lei Complementar 105/2001, de números 2.310, 2.397, 2.386 e 2.859.

Elas foram julgadas improcedentes, reconhecendo a constitucionalidade da Lei, e, assim, assentando o direito do Fisco de obter, independentemente de autorização judicial, informações bancárias dos contribuintes para fins de fiscalizar e cobrar tributos. Para o STF, a lei não autorizava a quebra, pois não autorizava a divulgação ou exposição dos dados:

> 4. Os artigos 5º e 6º da Lei Complementar nº 105/2001 e seus decretos regulamentares (Decretos nº 3.724, de 10 de janeiro de 2001, e nº 4.489, de 28 de novembro de 2009) consagram, de modo expresso, a permanência do sigilo das informações bancárias obtidas com espeque em seus comandos, não havendo neles autorização para a exposição ou circulação daqueles dados. (BRASIL, 2016)

A decisão reafirma que há transferência de informações entre portadores com obrigação legal de manter o sigilo das informações que tratam, confirmando a interpretação de que a norma é autorizadora daquilo que se convencionou chamar de "traslado de sigilo, ou seja, a ideia de que o sigilo não é quebrado quando há transferência dos dados entre duas autoridades governamentais, sendo ambas obrigadas a zelar pelo sigilo dos dados trasladados" (FEDERIGHI e CHOW, 2020, p. RR-12.5):

> Trata-se de uma transferência de dados sigilosos de um determinado portador, que tem o dever de sigilo, para outro, que mantém a obrigação de sigilo, permanecendo resguardadas a intimidade e a vida privada do correntista, exatamente como determina o art. 145, § 1º, da Constituição Federal. (BRASIL, 2016)

A decisão destaca ainda a importância dos dispositivos questionados como mecanismos de combate à sonegação fiscal, atendendo a padrões internacionais de transparência e de troca de informações:

> 5. [...] é preciso que se adotem mecanismos efetivos de combate à sonegação fiscal, sendo o instrumento fiscalizatório instituído nos arts. 5o e 6o da Lei Complementar n. 105/01 de extrema significância nessa tarefa.
>
> 6. O Brasil se comprometeu, perante o G20 e o Fórum Global sobre Transparência e Intercâmbio de Informações para Fins Tributários (Global Forum on Transparency and Exchange of Information for Tax Purposes), a cumprir os padrões internacionais de transparência e de troca de informações bancárias, estabelecidos com o fito de evitar o descumprimento de normas tributárias, assim como combater práticas criminosas. Não deve o Estado brasileiro prescindir do acesso automático aos dados bancários dos contribuintes por sua administração tributária, sob pena de descumprimento de seus compromissos internacionais". (BRASIL, 2016)

A decisão na ADI (FEDERIGHI e CHOW, 2020, p. RR-12.5) afirma também que o acesso das informações pelo Fisco não pode ser descartada em razão do dever fundamental de pagar tributos, reconhecendo que o acesso direto do Fisco aos dados financeiros dos

contribuintes é instrumento indispensável para a implementação do princípio da capacidade contributiva.

No mesmo julgamento, em uma segunda linha argumentativa, Toffoli justifica a legitimidade do Fisco para obter informações bancária dos contribuintes na razoabilidade, lembrando que, por imposição legal e sem necessidade de autorização judicial, o ente já possui acesso às informações do conjunto maior de patrimônio do contribuinte, que são declaradas à Receita Federal. Segundo Ávila e Woloszyn (2017, p. 191), "seria, assim, incongruente que o Fisco pudesse acessar o conjunto maior do patrimônio do contribuinte (bens e rendas) e não pudesse acessar o conjunto menor (movimentações financeiras)". Além disso, fica subentendido o princípio da eficiência quando o relator destaca que o instrumento fiscalizatório instituído nos artigos 5º e 6º da Lei Complementar nº 105/2001 "se mostra de extrema significância ao efetivo combate à sonegação fiscal no país" (BRASIL, 2016), sendo necessário para que o Estado cumpra seu papel de agente fiscalizador.

Em seu voto, acompanhando o voto do Relator pela constitucionalidade do acesso a dados bancários pelo Fisco independentemente de autorização judicial, o Min. Luís Roberto Barroso acrescenta que o sigilo de informações financeiras não se encontra no núcleo essencial do direito à intimidade, sendo, assim, passível de restrição razoável pelo legislador, principalmente com o objetivo de compatibilizá-lo com o dever fundamental de pagar tributos, a isonomia tributária e a capacidade contributiva.

O Min. Teori Zavaski, também acompanhando o Relator, acrescenta que todos os contribuintes já têm obrigação de fornecer informações bancárias ao Fisco no momento da declaração para o importo de renda,

> que serve de base para o ajuste anual, de modo que, ao se afirmar que há uma reserva de intimidade em relação a essas informações, ter-se-ia que afirmar que há uma reserva de intimidade também em relação às demais informações exigidas pelo Fisco (BRASIL, 2016).

Continua o Min. Zavaski que, no caso das pessoas jurídicas, não há que se falar em privacidade, uma vez que "elas têm obrigação de prestar contas não apenas ao Fisco, mas também à CVM ou aos seus acionistas, enfim, têm obrigação tornar públicas a grande maioria de sua situação patrimonial financeira" (BRASIL, 2016).

Destaca-se também a adoção pelos Ministros de uma série de argumentos pragmáticos (ÁVILA e WOLOSZYN, 2017, p.192) no sentido de que a decisão que estava sendo tomada seria "crucial para a efetiva repressão às organizações criminosas, ao narcotráfico, à lavagem

de dinheiro, ao terrorismo, não raro crimes de matiz internacional, tendo este último mostrado recentemente a sua face mais cruel nos atentados em Paris de novembro de 2015" (BRASIL, 2016b), conforme afirmou o então Presidente da Corte, Min. Lewandowski, em seu voto; ou então que a medida é salutar para otimizar a atividade fiscalizatória da Receita Federal nos termos "dos mais recentes compromissos internacionais assumidos pelo Brasil" (BRASIL, 2016) (voto do Min. Dias Toffoli).

Novamente no âmbito do STF, em decisão monocrática em 2016 no Recurso Extraordinário com Agravo nº 953.058, o Min. Gilmar Mendes afirmou a possibilidade de a Administração Fiscal encaminhar informações ao Ministério Público:

> [...] sendo legítimos os meios de obtenção da prova material e sua utilização no processo administrativo fiscal, mostra-se lícita sua utilização para fins da persecução criminal. Sobretudo, quando se observa que a omissão da informação revelou a efetiva supressão de tributos, demonstrando a materialidade exigida para configuração do crime previsto no art. 1º, inciso I, da Lei 8.137/1990, não existindo qualquer abuso por parte da Administração Fiscal em encaminhar as informações ao Parquet. (BRASIL, 2016)

Por sua vez, o Superior Tribunal de Justiça (STJ), em decisão de 2018, reconheceu, ao julgar o HC 422.473/SP, serem também válidos não apenas a requisição e o acesso às informações bancárias pelo Fisco e seu uso para fins de constituição do crédito tributário, mas também o compartilhamento desses dados, enquanto integrantes do processo administrativo fiscal, com a Procuradoria da Fazenda para fins de cobrança e com o Ministério Público para fins penais, entendendo ser "possível a utilização de dados obtidos pela Secretaria da Receita Federal, em regular procedimento administrativo fiscal, para fins de instrução processual penal" (BRASIL, 2018). Na mesma decisão, frisou que ocorre apenas transferência de dados entre entidades com dever de sigilo:

> [...] não há falar em ilicitude das provas que embasam a denúncia contra os pacientes, porquanto, assim como o sigilo é transferido, sem autorização judicial, da instituição financeira ao Fisco e deste à Advocacia-Geral da União, para cobrança do crédito tributário, também o é ao Ministério Público, sempre que, no curso de ação fiscal de que resulte lavratura de auto de infração de exigência de crédito de tributos e contribuições, se constate fato que configure, em tese, crime contra a ordem tributária (Precedentes do STF). (BRASIL, 2018)

As decisões analisadas demonstram que se encontra consolidado nas Cortes Superiores o entendimento de que o acesso por parte da Receita Federal aos dados bancários é não apenas permitido como necessário para o devido exercício de suas atribuições, seja no lançamento de

créditos tributários, ou como instrumento para a otimização do trabalho de fiscalização alinhado com as melhores práticas internacionais.

4.4 A LGPD E OS SIGILOS FISCAL E BANCÁRIO

O estudo dos sigilos fiscal e bancário leva-nos a concluir que a discussão sobre o tratamento de dados sigilosos/protegidos pela Receita Federal é antiga e madura, uma vez que as últimas alterações legais sobre os temas, por meio das Leis Complementares 104 e 105, completam 20 anos em 2021, além de já terem sido analisadas por diversas vezes pelo STJ e STF. Assim, dada a importância e impacto do início da vigência da LGPD sobre a disciplina de tratamento de dados pessoais como um todo, devemos nos debruçar sobre os seus efeitos nas discussões já travadas e analisar possíveis alterações ao que já se encontra estabelecido.

Advogando pela alteração do entendimento adotado pelo STF e STJ nos julgamentos das ações que tratam dos sigilos fiscal e bancário, analisadas nos itens 4.2 e 4.3, Federighi e Chow (2020, p. RR-12.15) defendem que deve haver uma interpretação integrativa das normas específicas sobre sigilo com a LGPD. Com a edição da norma, para os autores, seus efeitos vão além do Direito Privado, sendo aplicável também à Administração Pública, em especial na atividade de cobrança de tributos e à operação das instituições financeiras. Sendo a LGPD uma lei geral, sustentam que deveria haver coerência sistêmica entre ela e as leis específicas que regulam alguma questão do tratamento de dados. Concluem, assim, que os sigilos fiscal e bancário deveriam obedecer às regras e princípios previstos na LGPD, resultando no reconhecimento de que a transferência de dados por via administrativa seria ilegal e inconstitucional.

Os juristas iniciam sua análise reconhecendo que os sigilos fiscal e bancário não se encontram positivados no texto constitucional, mas, citando Gramstrup, que ambos possuem "supedâneo constitucional indireto" (GRAMSTRUP, 2014, p. 3-4) na intimidade e na vida privada, sendo delineados em normas infraconstitucionais.

Fazem tal afirmação porque os sigilos fiscal e bancário decorrem do direito à vida privada (o direito de indivíduos de resguardar em suas relações sociais a não divulgação de certas informações compartilhadas com essas pessoas), que é subespécie do Direito à Privacidade, de forma que a vinculação dos sigilos com a privacidade se estabelece, segundo Ávila e Woloszyn (2017, p.177), "à medida que os dados pessoais são documentos que contém informações sobre a vida privada de determinado indivíduo".

Dessa forma, decorreriam ambos, portanto, do direito à vida privada, pois há, no sigilo bancário, relação entre o indivíduo e a instituição financeira; e, no sigilo fiscal, relação entre o indivíduo e o Fisco, devendo as instituições resguardarem o não compartilhamento das movimentações bancárias e das declarações de imposto de renda, respectivamente. Ademais, as informações bancárias e fiscais possuem caráter individual e relativo exclusivamente à pessoa física que realiza as movimentações, se enquadram na definição de dados pessoais e, consequentemente, se encontrariam protegidos pela LGPD. Isso porque, segundo o inciso I, artigo 5º da Lei Geral de Proteção de Dados, dado pessoal consiste em informação relacionada à pessoa natural identificada ou identificável (GREGÓRIO e MELO, 2020).

Assim, para Federighi e Chow (2020, p. RR-12.4), teríamos o mesmo bem jurídico, a privacidade, tutelado sob roupagens diferentes: no sigilo bancário, a vida privada se garante por meio de uma relação de confiança na não divulgação de dados por entidades privadas, enquanto no sigilo fiscal o mesmo bem jurídico o é por meio de uma proibição à conduta estatal.

Como analisado nas decisões do STF, nenhum dos direitos é absoluto: ambos devem ser preservados até que ocorra uma situação que justifique sua quebra. A violação dos sigilos bancário e fiscal deveriam então ser entendidos como um caso excepcional, que necessitaria de uma autorização judicial bem fundamentada, a exemplo da parte final do inciso XII do artigo 5º, que incluiu uma possibilidade de retirar do âmbito da inviolabilidade o sigilo das comunicações telefônicas. Para os juristas (FEDERIGHI e CHOW, 2020, p. RR-12.4), os sigilos deveriam ter a mesma proteção apesar de não possuírem a mesma previsão constitucional expressa. Esse já fora o entendimento do STJ, conforme decidido em 2005 no Recurso em Mandado de Segurança 15.364/SP:

> [...] a proteção aos sigilos bancário e fiscal não é direito absoluto, podendo ser quebrados em casos excepcionais e em razão de decisão fundamentada, quando presentes circunstâncias que denotem a existência de interesse público relevante ou de elementos aptos a indicar a possibilidade de prática delituosa. (BRASIL, 2005)

Reforçaria esse entendimento o artigo 145, § 1º, que possibilita a implementação pela administração tributária de obrigações acessórias ou deveres instrumentais que sejam utilizados para identificar de maneira mais apurada possível o patrimônio, os rendimentos e as atividades econômicas do contribuinte. Condiciona, entretanto, que essa atividade deve respeitar os direitos individuais e os termos da lei, fazendo remissão, portanto, aos direitos de privacidade previstos no artigo 5º como direitos fundamentais.

Assim, para os autores, o Direito brasileiro dá subsídios para se poder entender como as normas relativas aos sigilos fiscal e bancário devem se relacionar interpretativamente com a LGPD. Tanto os direitos de autodeterminação informacional (fundamento da LGPD) quanto os direitos a sigilo fiscal e bancário estão previstos constitucionalmente no artigo 5º como Direitos Fundamentais relacionados a uma "macroideia de privacidade" (FEDERIGHI e CHOW, 2020, p. RR-12.11), ou seja, decorrem de uma mesma fonte. Soma-se a isso as determinações da LGPD sobre o tratamento de dados, em que o compartilhamento é uma das formas de tratamento previstas pela lei (conforme o seu art. 5º).

Tendo em vista que as informações de natureza bancária e fiscal possuem caráter individual relacionado à pessoa física responsável pelas movimentações financeiras, elas se enquadram na definição de dados pessoais. A partir disso, os juristas afirmam que foi um erro da LGPD não ter incluído no rol de dados pessoais sensíveis (art. 5º, II) os dados fiscais, uma vez que

> traduzem a situação financeira do indivíduo, que corresponde a direito da personalidade: esses dados dizem muito de nós, pois se referem a nossas movimentações financeiras, que podem ser traduzidas em padrões de consumo, gastos de vida, de transferências bancárias entre pessoas físicas ou jurídicas, logo, são informações que dizem respeito à rotina, à privacidade e ao patrimônio. (SARDENBERG, 2019, apud FEDERIGHI e CHOW, 2020, p. RR-12.12)

Assim, concluem Federighi e Chow (2020, p. RR-12.14) que a previsão de compartilhamento de dados fiscais pela Lei Complementar 104/2001 e de dados bancários da Lei Complementar 105/2001 seria tanto inconstitucional quanto ilegal, tendo em vista que a LGPD é a lei geral e principiológica que regula o tratamento de dados pessoais, que incluem os dados fiscais e bancários. Haveria a necessidade de observância dos princípios do artigo 6º da LGPD no compartilhamento, que leva à necessidade de autorização judicial baseada em fundamento relevante, não sendo possível a transferência administrativa, sem a devida autorização judicial.

Fernandes (2019) possui um entendimento diferente de Federighi e Chow, e a favor da manutenção do entendimento estabelecido sobre os sigilos fiscal e bancário, por concluir ser uma discussão distinta daquela provocada pela LGPD. Comparando-se as informações prestadas ao Fisco e aquelas compartilhadas com terceiros com quem as empresas possuem relações jurídicas, o jurista identifica dados que a Administração Federal necessita para cumprir sua função legal, mas que, se compartilhadas com terceiros, poderiam descumprir as

determinações da Lei Geral de Proteção de Dados. Para ele, isso é evidência de que tratam de situações e tratamentos de dados distintos, sob a tutela de normas diferentes.

Como exemplo, cita a Escrituração Digital das Obrigações Fiscais, Previdenciárias e Trabalhistas (eSocial), que exige que as empresas prestem extensa quantidade de informações sobre todos os empregados e trabalhadores autônomos contratados por ela. Considerando que o cadastro do eSocial é bastante completo, a administração das empresas poderia compartilhar esses mesmos dados com outros interessados, como um banco, por exemplo. “Acontece que os dados informados no eSocial são superiores, em quantidade e qualidade, àqueles necessários em outras relações contratuais” (FERNANDES, 2019).

Assim haveria divulgação indevida dos dados pessoais dos funcionários, que estão sob o manto da Lei Geral de Proteção de Dados, mas devem ser informadas à administração fiscal, delimitando e distanciando o âmbito de atuação da LGPD e das leis específicas que tratam dos sigilos fiscal e bancário. Desse modo,

> quando se trata de informações e dados de pessoas, quer físicas quer jurídicas, não é possível "cortar e colar" os cadastros e demais informações prestadas ao Fisco. Na relação tributária, existe o sigilo fiscal; nas relações privadas, aplica-se a LGPD. (FERNANDES, 2019)

Acrescenta-se à discussão a decisão proferida pelo plenário do STF no julgamento do Recurso Extraordinário 1055941, com repercussão geral reconhecida (Tema 990). Trata o recurso de ação penal anulada pelo Tribunal Regional Federal da 3ª Região Fiscal diante do compartilhamento, para fins penais, com o Ministério Público de dados obtidos pela Receita Federal.

O plenário reverteu a decisão liminar do então presidente do STF, Ministro Dias Toffoli, que havia determinado a suspensão de todas os processos judiciais em andamento no país que versassem sobre o compartilhamento, sem autorização judicial e para fins penais, de dados fiscais e bancários do contribuinte (BRASIL, 2019). Na decisão de 28/11/2019, o plenário do STF se manifestou no sentido de que é legítimo o compartilhamento com o Ministério Público e as autoridades policiais, para fins de investigação criminal, da integridade dos dados bancários e fiscais do contribuinte obtidos pela Receita Federal e pela Unidade de Inteligência Financeira (UIF), sem a necessidade de autorização prévia do Poder Judiciário.

O entendimento que justificou tal decisão está sedimentado no STF desde o julgamento da ADI 2.859 bem como encontra fundamento na própria LGPD, que discorre a respeito das hipóteses em que os dados, mesmo que pessoais, não terão seu tratamento restringido

(GREGÓRIO e MELO, 2020). De acordo com o inciso III, artigo 4º da LGPD, não se aplica a referida norma ao tratamento de dados pessoais realizado para fins exclusivos de a) segurança pública; b) defesa nacional; c) segurança do Estado; ou d) atividades de investigação e repressão de infrações penais.

No caso analisado no RE 1055941, o compartilhamento de dados bancários e fiscais, obtidos pela Receita Federal e pelo UIF, ao Ministério Público e à polícia investigativa têm por objetivo principal evitar que o sistema financeiro seja um meio para a prática de infrações penais, de forma que se encontram enquadradas na exceção do art. 4º da LGPD, dispositivo que visa proteger a eficácia das investigações e a segurança pública. Dessa forma, do ponto de vista da nova norma de proteção de dados, o compartilhamento de informações bancárias e fiscais, no caso em apreço, é possível e a decisão da Corte, tomada antes da entrada em vigência da LGPD, está em harmonia com esta, dispensando a necessidade de eventual rediscussão do tema.

Por todo o exposto, em que pese a excelente análise conduzida por Federighi e Chow em seu trabalho, entende-se que a edição da Lei Geral de Proteção de Dados não alteram as normas e jurisprudência estabelecidas acerca dos temas sigilo fiscal e sigilo bancário, relacionados à essência do tratamento de dados feito pela Receita Federal no cumprimento de sua função institucional.

O acesso dos Fiscos à intimidade, conforme analisado nos itens anteriores, se mostra medida necessária ao cumprimento da justiça fiscal, materializado no §1º do art. 145 da Constituição Federal, que determina que sempre que possível, os impostos terão caráter pessoal e serão graduados segundo a capacidade econômica do contribuinte.

Reforça ainda a necessidade de uso e compartilhamento de dados dos contribuintes a indicação no art. 37, inciso XXII, da Constituição, de que as administrações tributárias da União, dos Estados, do Distrito Federal e dos Municípios atuarão de forma integrada, inclusive com o compartilhamento de cadastros e de informações fiscais.

Ademais, o Supremo Tribunal Federal acertadamente sedimentou a jurisprudência de que as informações prestadas por instituições financeiras à Receita Federal estão entre as que esta deve acessar para cumprir sua competência legal e não configuram uma autorização para liberação indiscriminada dessas informações a terceiros, encontrando-se o procedimento, portanto, alinhado à LGPD. Acertou também a Corte em reconhecer a possibilidade de compartilhamento de informações do Fisco Federal com o Ministério Público, titular da investigação e repressão de infrações penais, medida também alinhada à LGPD.

4.5 BOAS PRÁTICAS E GOVERNANÇA NO TRATAMENTO DE DADOS PESSOAIS

Importante dispositivo da Lei Geral de Proteção de Dados — possivelmente o mais importante para as entidades da administração pública, e consequentemente para a Receita Federal — é o que trata das boas práticas e das medidas de governança dos dados. Essas medidas visam impedir que dados pessoais sejam acessados e expostos indevidamente.

A governança de dados tem o propósito de coordenar, orientar e definir regras para a criação, coleta e uso de dados, visando garantir a segurança no armazenamento, monitoramento e geração de dados (POLONI, 2019). Ela se ocupa dos dados estratégicos da organização, definindo e analisando os processos que produzem e usam esses dados (BARBOSA e LYRA, 2019).

Para a plataforma do Governo Digital,

> é a gestão de dados na esfera de alto nível, ou seja, é o exercício de autoridade e controle, relacionado ao planejamento, monitoramento e execução, sobre a gestão de ativos de dados de modo a promover a interoperabilidade das informações, meios de análise de políticas públicas e serviços digitais mais simples e ágeis ao cidadão, organizações e empresas. (BRASIL, 2019)

A LGPD regulamenta também a forma como a Administração Pública (e qualquer entidade, pública ou privada, que faça algum tratamento de dados pessoais) cuida dos dados que coleta e utiliza no cumprimento de suas atribuições legais. Nas palavras de Lacet (2019),

> a inclusão do setor público no escopo da LGPD constitui um marco na Administração Pública, obrigando-a a se adequar e investir em questões de segurança e a atuar de forma a evitar a utilização de dados pessoais para fins diferentes daqueles para os quais foram coletados, considerando que os governos têm se tornado cada vez mais digitais, além de serem os maiores detentores de dados pessoais. (LACET, 2019)

A autora reforça que a LGPD não impede o setor público do tratamento de dados pessoais, "até porque é uma atividade necessária e inerente à consecução das inúmeras políticas públicas que desempenha" (LACET, 2019). Entretanto, a administração terá que se adaptar aos princípios da Lei e se adaptar aos novos deveres que estipula, pois

> apesar da necessidade de regulamentação de vários dispositivos para a implementação das regras de conformidade da LGPD no setor público, é certo que a administração pública necessitará investir em três pilares: Tecnologia, para instituir uma política forte de segurança em TI, com atenção ainda maior para que as aplicações que tratam com dados pessoais estejam seguras desde a concepção; Processos, mapeando-os para entender todo o fluxo do tratamento de dados e identificar os riscos inerentes ao

> tratamento; e Pessoas, capacitando-as e conscientizando-as da importância em estar e permanecer em conformidade com a lei. (LACET, 2019)

A orientação para os cuidados necessários no tratamento de dados pessoais são indicadas na LGPD em sua Seção II, intitulada Das Boas Práticas e da Governança, que estimula a formulação de regras de boas práticas e de governança a serem estabelecidas pelos controladores e operadores pelo tratamento de dados pessoais. *In* v*erbis:*

> Art. 50. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais (BRASIL, 2018).

O Art. 50, §2º da LGPD estabelece as características mínimas de um programa de governança em privacidade. Este deve a) demonstrar 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; que b) seja aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta; que c) seja adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados; que d) estabeleça políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade; que 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; que f) esteja integrado a sua estrutura geral de governança e estabeleça e aplique mecanismos de supervisão internos e externos; que g) conte com planos de resposta a incidentes e remediação; e que h) seja atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas.

Com o início da vigência da LGPD, o Governo Federal, por meio da Secretaria de Governo Digital, preparou guias para orientar a implantação da LGPD no âmbito federal, intitulados Guia de Boas Práticas – Lei Geral de Proteção de Dados e Guia de Elaboração de Programa de Governança em Privacidade. A iniciativa faz parte do esforço para oferecer digitalmente 100% dos mais de 3 mil serviços da União (BRASIL, 2020) que está materializada na Estratégia de Governo Digital para o período de 2020 a 2022, instituído pelo Decreto nº 10.332, de 28 de abril de 2020.

O Guia de Boas Práticas – Lei Geral de Proteção de Dados tem como objetivo "fornecer orientações de boas práticas aos órgãos e entidades da Administração Pública Federal direta, autárquica e fundacional para as operações de tratamento de dados pessoais, conforme previsto no art. 50 da LGPD" (BRASIL, 2020, p.8).

Por sua vez, o Guia de Elaboração de Programa de Governança em Privacidade "orienta a elaboração de um Programa de Governança em Privacidade por órgãos e entidades da administração Pública Federal (APF) direta, autárquica e fundacional" (BRASIL, 2020, p. 6). Ele determina que o programa deve estabelecer uma metodologia abrangente, que influenciará permanentemente os processos de tomada de decisão relacionados ao tratamento de dados pessoais. Para tanto, o programa deve ser estruturado em etapas, que abrangem a sua iniciação e planejamento, a sua construção e execução e, por fim, o seu monitoramento. Essas etapas devem ser executadas em um ciclo permanente, de constante aperfeiçoamento da governança dos dados pessoais.

Na iniciação e planejamento devem os órgãos "buscar compreender quais são as primeiras informações e dados importantes que devem ser conhecidos" (BRASIL, 2020, p. 10). Essa etapa deve ser iniciada pela nomeação do Encarregado, que conforme o art. 5º, inciso VIII da LGPD, é a pessoa indicada pelo operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a ANPD. Sua função é importante para a implementação da LGPD e do Programa de Governança em Privacidade.

Ao longo da etapa de Iniciação e Planejamento devem ser alinhadas as expectativas com a alta administração do órgão (Ministros de Estado, ocupantes de cargos de natureza especial e chefias). Deve também ser analisada a maturidade da organização, com o intuito de identificar o estágio de adequação dos processos de tratamento de dados à LGPD (BRASIL, 2020, p. 14). Nessa etapa devem ainda ser analisadas as medidas de segurança existentes para proteção dos dados pessoais, com vistas a evitar acessos não autorizados ou qualquer forma de tratamento inadequado ou ilícito. É recomendado ainda o estabelecimento de uma estrutura organizacional para governança e gestão da proteção de dados pessoais; e o inventário dos dados pessoais utilizados pelo órgão, em que são mapeados e documentados os tratamentos de dados pessoais realizados pela instituição e, segundo o Guia, "consiste em uma excelente forma de fazer um balanço do que o órgão e entidade faz com os dados pessoais, identificando quais dados pessoais são tratados, onde estão e que operações são realizadas com eles" (BRASIL, 2020, p. 16).

Na etapa seguinte, construção e execução do programa, deve-se garantir que os usos dos dados pessoais sejam conhecidos e adequados de acordo com as leis, bem como sua proteção contra mau uso ou revelação inadvertida ou deliberada. Assim, são gerenciados os direitos

individuais de privacidade, como o direito de acessar os dados que um órgão ou entidade mantém sobre os indivíduos, o direito de os atualizar, devendo os órgãos estarem preparados para receber, realizar a triagem e responder consultas e reclamações. Deve haver controle do consentimento e rastreamento de preferência, que implica em o órgão estar posicionado para capturar consentimento e rastrear solicitações de preferências tanto dos titulares dos dados como dos agentes de tratamento, o que ajudar a reduzir a probabilidade de problemas e aumenta a confiança do cidadão. Por fim, devem ser adotadas medidas que reduzam a exposição a riscos, como, por exemplo, a criptografia e anonimização de dados e a manutenção dos dados apenas para sua finalidade (BRASIL, 2020, p. 17)

Na última etapa, o monitoramento do programa é a forma de acompanhar sua conformidade à LGPD, e deve ser atividade contínua. Essa etapa engloba atividades de coleta e análise de informações, elaboração de relatórios e apresentações de resultados. Nessa etapa são utilizados indicadores de performance, que ajudam a monitorar e acompanhar fatos importantes na gestão do programa, como o número de incidentes de violação de dados pessoais e/ou vazamento de dados pessoais, índice de adequação à LGPD, índice de quantidade de treinamentos realizados para conscientizar os agentes e outros. É feita também uma gestão de incidentes, que descreva, armazene, faça análises de informações sobre incidentes ou eventos e gerencie os riscos relacionados e as medidas tomadas. Por fim, a elaboração de reportes dos resultados, que demonstrem a evolução das ações e resultados obtidos (BRASIL, 2020, p. 25-26).

5 CONSIDERAÇÕES FINAIS

Este trabalho buscou analisar a situação do tratamento de dados pela Receita Federal após a edição da Lei Geral de Proteção de Dados: de que forma o novo normativo impacta e interfere na análise que o Fisco Federal faz dos dados pessoais e sigilosos dos contribuintes e como as novas regras se harmonizam com aquelas já estabelecidas.

O tema do tratamento de dados pessoais ganhou mais atenção com as inovações tecnológicas que potencializaram a capacidade de coleta e armazenamento de dados pessoais, e o consequente aumento do risco de uso e divulgação indevidos dessas informações. Nesse contexto, foi editada a importante Lei Geral de Proteção de Dados, que estabelece as bases da disciplina da proteção de dados pessoais no ordenamento jurídico brasileiro e é influenciada pela discussão internacional. Estando o trabalho da Receita Federal apoiado na coleta e uso intensivo de dados pessoais e privados/íntimos dos contribuintes, se mostra importante analisar os impactos da entrada em vigor da Lei nos trabalhos de análise de informações protegidas pelos sigilos fiscal e bancário.

O estágio atual da disciplina de proteção de dados pessoais é fruto de longa discussão internacional sobre o tema, que estabeleceu os fundamentos que orientaram a edição da norma brasileira, fortemente inspirada no Regulamento Europeu (GDPR). Antes da edição da LGPD, pouca discussão foi identificada no ordenamento brasileiro, podendo-se apontar apenas dispositivos muito específicos sobre o tema, como a previsão constitucional do *Habeas Data*, artigos no Código de Defesa do Consumidor e a Lei de Acesso à Informação, entre outros.

Para a devida compreensão da realidade atual das discussões, o estudo inicia na análise da evolução histórica do direito da privacidade, que recentemente assumiu contornos mais voltados à tutela dos dados pessoais. Chama atenção nessa parte do estudo a pouca discussão no Brasil sobre o direito à privacidade, concentrando-se o estudo em importantes debates que ocorreram nos EUA e na Europa.

Os debates sobre a proteção de dados pessoais ganharam força na década de 60 e as normas passaram por gerações, sendo que primeiras surgiram em reação a iniciativas governamentais que propunham concentrar em um único local toda a informação disponível em bases de dados públicas sobre os cidadãos. Esses projetos geraram reações negativas, não foram implementados e ainda deram origem a normas que restringiam a concentração de dados pessoais por parte das administrações públicas dos países.

É realizado, então, o estudo da experiência europeia, cuja legislação mais recente, o Regulamento Geral sobre Proteção de Dados (GDPR) foi a principal referência quando da elaboração da LGPD. A legislação europeia passou por diversas normas, destacando-se a Convenção 108/1981, específica para tratar da proteção de dados pessoais, cujo propósito foi estimular os estados-membros da Comunidade Europeia a adotar normas para a tutela de dados pessoais.

A uniformização normativa da proteção de dados na Europa só foi alcançada com a edição do Regulamento Geral de Proteção de Dados, em vigência hoje. A GDPR é norma rígida, aplicável a qualquer empresa que processe dados de cidadãos europeus, ainda que não localizada na Europa. Ela estabelece ainda regras de consentimento para o processamento de informações e diversos direitos para os titulares dos dados terem amplo controle sobre o uso de suas informações.

Essa primeira etapa do trabalho é concluída com uma análise da experiência brasileira anterior à LGPD. Ela é pequena, destacando-se a previsão constitucional do *Habeas Data*, que estabelece uma modalidade de direito de acesso e retificação dos dados pessoais e, na legislação ordinária, destaca-se os dispositivos do Código de Defesa do Consumidor que trazem direitos e garantias para o consumidor em relação às suas informações pessoais presentes em bancos de dados e cadastros.

Assumindo a tarefa de estabelecer a disciplina e as bases da discussão do tratamento de dados pessoais, a LGPD indica em seus artigos iniciais o seu alcance, fundamentos, os tipos de operações que orienta, exceções à sua aplicação, conceitos básicos da disciplina e princípios que a atividade de tratamento de dados pessoais deve observar. Em capítulo específico, trata ainda das regras do tratamento de dados pessoais pelo poder público. A Lei prevê que as entidades da Administração Pública poderão, para cumprimento de sua obrigação legal, realizar tratamentos de dados pessoais, desde que obedecidas regras específicas sobre o uso e compartilhamento dos dados, estando sujeitas às normas da Autoridade Nacional de Proteção de Dados. As entidades, em caso de infrações cometida às normas previstas na Lei, estão ainda sujeitas a diversas sanções.

Do ponto de vista da Receita Federal, destaca-se os dispositivos que possibilitam o tratamento de dados pessoais nas atividades de investigação e repressão de infrações penais (art. 4º, III, d), e o artigo 7º, inciso III, que estabelece as hipóteses em que o tratamento de dados poderá ser realizado pela administração pública, para tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres.

Do capítulo específico para o poder público, destaca-se a previsão do artigo 23, que na parte final do seu caput autoriza o tratamento de dados pessoais que tiver como objetivo a execução das competências legais ou para cumprir as atribuições legais do serviço público. Em razão do princípio da legalidade, qualquer órgão público está sempre amparado em uma disposição legal em suas ações, o que acaba por fundamentar, em algum nível, o tratamento de dados pessoais, quando executado dentro de suas competências legais.

Analisou-se, então, a situação atual da discussão sobre o acesso da Receita Federal a informações sigilosas, em especial os sigilos fiscal e bancário, e dos debates em torno dos dois temas. Constatou-se que o entendimento atual foi alcançado após repetidas ações julgadas pelas Cortes Superiores, que reconhecem a pertinência do acesso pelo Fisco dessas informações para cumprimento de sua obrigação legal. Demonstra-se ainda a discussão das consequências da edição da LGPD para esse acesso, em que foi identificado posicionamento que advoga pela revisão das decisões que reconheciam a sua legalidade. Após enumeração de posicionamentos a favor e contra a mudança do entendimento da jurisprudência, conclui-se que a edição da LGPD não altera os argumentos que embasaram as decisões e que o acesso da Receita Federal às informações sigilosas permanece autorizado.

Por fim, apesar de se concluir que a LGPD não altera a substância das regras que disciplinam o acesso do Fisco Federal a dados sigilosos dos contribuintes, ela traz dispositivos que determinam a formulação de regras de boas práticas e de governança para aqueles responsáveis pelo tratamento dos dados. Essas regras exigem a adoção de procedimentos para garantir a proteção das bases mantidas pelo Poder Público, com intuito de impedir o acesso indevido por terceiros. Estuda-se, então, os Guias publicados pela plataforma do Governo Digital, que orientam o estabelecimento dos processos de governança de dados a serem adotados pelas entidades da administração pública federal.

REFERÊNCIAS

ALVES, Fabricio da Mota. **Capítulo VIII – Da Fiscalização**. In: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (coord.). LGPD: Lei Geral de Proteção de Dados: comentada. 2. ed. rev. atual. e ampl. São Paulo: Revista dos Tribunais, 2019. 574 p.

ARAÚJO, Alexandra Maria Rodrigues.; OLIVEIRA, José Sebastião de. **As transferências de dados pessoais para países terceiros acompanhada de uma decisão de adequação no direito da união europeia**. Direito e novas tecnologias I. CONPEDI 2014. Disponível em: < http://publicadireito.com.br/artigos/?cod=5b8f9c769baebee0 >. Acesso em 31/03/2021.

ÁVILA, Ana Paula Oliveira; WOLOSZYN, André Luis. **A tutela jurídica da privacidade e do sigilo na era digital: doutrina, legislação e jurisprudência**. Rev. Investig. Const., Curitiba, v. 4, n. 3, dez. 2017. p. 171. Disponível em: <http://www.scielo.br/pdf/rinc/v4n3/2359-5639-rinc-04-03-0167.pdf>. Acesso em: 18.03.2021

BARBOSA, Wellington Luiz; LYRA, Roberto Shayer. **Governança de Dados. Módulo 1. Contexto da Governança de Dados na Administração Pública**. Brasília, 2019. Disponível em: < https://repositorio.enap.gov.br/bitstream/1/5008/1/M%c3%b3dulo%201%20-%20Contexto%20da%20Governan%c3%a7a%20de%20Dados%20na%20Administra%c3%a7%c3%a3o%20P%c3%bablica.pdf >Acesso em 31/03/2021.

BARROSO, Luís Roberto Barroso; BARCELLOS, Ana Paula. **A viagem redonda: Habeas Data, direitos constitucionais e as provas ilícitas**. Revista Dir. Adm. Rio de Janeiro, 213: 149-163. Jul./set. 1998. Disponível em: < http://bibliotecadigital.fgv.br/ojs/index.php/rda/article/view/47206/45406 >. Acesso em 31/03/2021.

BRASIL. **Lei Federal nº 8.078, de 11 de setembro de 1990**. Dispõe sobre a proteção do consumidor e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 24/02/2021.

_____. Lei 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados**. Disponível em < http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm >. Acesso em 25/02/2021.

_____. Lei Federal nº 8.078, de 11 de setembro de 1990. **Código de Defesa do Consumidor**. Disponível em: < http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm >. Acesso em 24/02/2021.

_____. Lei 10.406, de 10 de janeiro de 2002. **Código Civil**. Disponível em < http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm>. Acesso em 04/03/2021.

_____. Lei 12.527, de 18 de novembro de 2011. **Lei de Acesso à Informação**. Disponível em <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm>. Acesso em 06/03/2021.

_____. Lei 12.965, de 23 de abril de 2014. **Marco Civil da Internet**. Disponível em <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em 08/03/2021.

_____. Decreto 8.771, de 11 de maio de 2016. **Decreto de Regulamentação do Marco Civil da Internet**. Disponível em <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/D8771.htm>. Acesso em 08/03/2021.

_____. Lei 9.610, de 19 de fevereiro de 1998. **Altera, atualiza e consolida a legislação sobre direitos autorais e dá outras providências**. Disponível em <http://www.planalto.gov.br/ccivil_03/leis/l9610.htm>. Acesso em 11/03/2021.

_____. Decreto-Lei 4.657, de 4 de setembro de 1942. **Lei de Introdução às normas do Direito brasileiro**. Disponível em <http://www.planalto.gov.br/ccivil_03/decreto-lei/del4657.htm>. Acesso em 15/03/2021.

_____. Decreto nº 8.842, de 29 de agosto de 2016. **Promulga o texto da Convenção sobre Assistência Mútua Administrativa em Matéria Tributária emendada pelo Protocolo de 1º de junho de 2010, firmada pela República Federativa do Brasil em Cannes, em 3 de novembro de 2011.** Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/D8842.htm >. Acesso em 27/03/2021.

_____. Lei 8.112, de 11 de dezembro de 1990. **Dispõe sobre o regime jurídico dos servidores públicos civis da União, das autarquias e das fundações públicas federais**. Disponível em: < http://www.planalto.gov.br/ccivil_03/leis/l8112cons.htm >. Acesso em 27/03/2021.

_____. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. **Código Penal**. Disponível em: < http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm >. Acesso em 27/03/2021.

_____. Superior Tribunal de Justiça. **Habeas Corpus nº 160.646/SP**. Disponível em < https://processo.stj.jus.br/processo/revista/documento/mediado/?componente=ATC&sequencial=17084731&num_registro=201000151383&data=20110919&tipo=5&formato=PDF >. Acesso em 27/03/2021.

_____. Supremo Tribunal Federal. **Recurso Extraordinário 601.314/SP**. Disponível em < http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=11668355>. Acesso em 28/03/2021.

_____. Supremo Tribunal Federal. **ADI 2859/DF**. Disponível em < http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=11899965 >. Julgada em 24/02/2016. Publicada em 21/10/2016. Acesso em 28/03/2021.

_____. Supremo Tribunal Federal. **ARE/953058**. Disponível em < http://stf.jus.br/portal/diarioJustica/verDiarioProcesso.asp?numDj=109&dataPublicacaoDj=30/05/2016&incidente=4939303&codCapitulo=6&numMateria=79&codMateria=3 >. Decisão de 25/05/2016. Acesso em 28/03/2021.

_____. Superior Tribunal de Justiça. **HC 422.473/SP**. Disponível em < https://www.stj.jus.br/websecstj/cgi/revista/REJ.cgi/ITA?seq=1691355&tipo=0&nreg=201702800289&SeqCgrmaSessao=&CodOrgaoJgdr=&dt=20180327&formato=PDF&salvar=false >. Julgada em 20/03/2018. Publicada em 27/03/2018. Acesso em 28/03/2021.

_____. Superior Tribunal de Justiça. **RMS 15364/SP**. Disponível em < https://stj.jusbrasil.com.br/jurisprudencia/7193454/recurso-ordinario-em-mandado-de-seguranca-rms-15364-sp-2002-0121341-5/inteiro-teor-12938186>. Julgada em 06/09/2005. Publicada em 10/10/2005. Acesso em 28/03/2021.

_____. Supremo Tribunal Federal. **RE 1055941/SP**. Disponível em < http://portal.stf.jus.br/processos/detalhe.asp?incidente=5213056 >. Decisão de 28/11/2019. Acesso em 28/03/2021.

_____. **Guia de Elaboração de Programa de Governança em Privacidade, Lei Geral de Proteção de Dados Pessoais (LGPD)**. Versão 1.0. Brasília, outubro de 2020. Disponível em: < https://www.gov.br/governodigital/pt-br/governanca-de-dados/GuiaProgramaGovernanaemPrivacidade.pdf >. Acesso em 25/03/2021.

_____. **Guia de Boas Práticas Lei Geral de Proteção de Dados (LGPD)**. Versão 2.0. Brasília, agosto de 2020. Disponível em: < https://www.gov.br/governodigital/pt-br/governanca-de-dados/GuiaLGPD.pdf >. Acesso em 25/03/2021.

_____. **O que é? Governança de dados**. Publicado em 27/11/2019. Atualizado em 25/01/2021. Disponível em: < https://www.gov.br/governodigital/pt-br/governanca-de-dados >. Acesso em 31/03/2021.

_____. Decreto nº 10.332, de 28 de abril de 2020. **Institui a Estratégia de Governo Digital para o período de 2020 a 2022, no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional e dá outras providências**. Disponível em < http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2020/Decreto/D10332.htm >. Acesso em 31/03/2021.

BLUM, Renato Opice, LÓPEZ, Nuria. **Lei Geral de Proteção de Dados no setor público: transparência e fortalecimento do Estado Democrático de Direito**. In: Cadernos Jurídicos da Escola Paulista da Magistratura, São Paulo, ano 21, nº 53, p. 171-177, Janeiro-Março/2020.

CACHAPUZ, Maria Cláudia Mércio. **Privacidade, proteção de dados e autodeterminação informativa.** Revista Jurídica da Presidência Brasília v. 15 n. 107. Out. 2013/Jan. 2014 p. 823 a 848. Disponível em: < https://revistajuridica.presidencia.gov.br/index.php/saj/article/view/126/118 >. Acesso em 31/03/2021.

CANCELIER, Mikhail Vieira de Lorenzi. **O Direito à Privacidade hoje: perspectiva histórica e o cenário brasileiro**. Sequência (Florianópolis), Florianópolis, n. 76, p. 213-239, Maio de 2017. Disponível em <http://www.scielo.br/scielo.php?script=sci_arttext&pid=S2177-70552017000200213&lng=en&nrm=iso>. Acesso em 31/03/2021.

COTS, Márcio; OLIVEIRA, Ricardo. **Lei Geral de Proteção de Dados Pessoais: comentada.** Prefácio: Danilo Doneda. 3. ed. rev. atual. e ampl. São Paulo: Revista dos Tribunais, 2020. E-book. 318 p.

DALLARI, Dalmo de Abreu. **O Habeas-Data no sistema jurídico brasileiro.** 2002. Disponível em: < https://dialnet.unirioja.es/descarga/articulo/5085310.pdf >. Acesso em 31/03/2021.

DONEDA, Danilo Cesar Maganhoto. **Da privacidade à proteção de dados pessoais: elementos da formação da Lei Geral de Proteção de Dados**. 2ª ed. São Paulo: Thomson Reuters Brasil, 2020. E-book (não paginado).

FEDERIGHI, André Catta Preta; CHOW, Beatriz Graziano. **Os sigilos fiscal e bancário e a LGPD: direito fundamental à autodeterminação informacional no âmbito do Direito Tributário.** Revista de Direito Bancário e do Mercado de Capitais, São Paulo, v. 23, n. 89, jul./set. 2020.

FERNANDES, Bernardo Gonçalves. **Curso de Direito Constitucional**. 9ª ed. rev., ampl. e atual. Salvador: JusPODIVM, 2017.

FERNANDES, Edison Carlos. **O que a declaração tributária tem a ver com a proteção de dados.** Disponível em: [www.migalhas.com.br/depeso/304598/o-que-a -declaracao-tributaria-tem-a-ver-com-a-protecao-de-dados]. Acesso em 23/03/2021.

FRANÇA. Act nº 78-17 de 6 de janeiro de 1978. **Loi Informatique et Libertes**. Disponível em <https://www.cnil.fr/sites/default/files/typo/document/Act78-17VA.pdf>. Avesso em 25/02/202.

GRAMSTRUP, Erik Frederico. **Sigilo fiscal e bancário: fundamentos normativos e principiológicos da quebra**. Revista Brasileira de Estudos Constitucionais, Belo Horizonte, ano 8, n. 28, jan.-abr. 2014. Disponível em < https://www.academia.edu/download/38628448/sigilo_fiscal_e_bancario_artigo_erik_f_gramstrup_-_revisto_03_2014_-_indicacao_revista.pdf >. Acesso em 20/03/2021.

GREGÓRIO, João Paulo; MELO, Isadora Sagmeister de. **A relação entre o compartilhamento dos dados bancários e fiscais do contribuinte obtidos pela Receita Federal sem autorização judicial e a Lei Geral de Proteção de Dados**. Disponível em: [www.migalhas.com.br/depeso/323510/a-relacao-entre-o-compartilhamento-dos-dados-bancarios-e-fiscais-do-contribuinte-obtidos-pela-receita-federal-sem-autorizacao-judicial-e-a-lei-geral-de-protecao-de-dados]. Acesso em: 19/03/2021.

FRAZÃO, Ana. TEPEDINO, Gustavo. OLIVA, Milena Donato. **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito brasileiro**. coordenação. – 1. ed – São Paulo: Thomson Reuters Brasil, 2019.

LACET, Érika. **LGPD e os impactos na Administração Pública**. 25/10/2019 Disponível em: [www.conaci.org.br/artigos/lgpd-e-os-impactos-na-administracao-publica]. Acesso em: 23.03.2021.

MACHADO, E. D.; JANINI, T. C. **O sigilo fiscal e a lei de acesso à informação:**

possibilidades de acesso à informação administrativa fiscal. Prisma Jurídico, São Paulo, v. 14, n. 2, p. 9-31, jul./dez. 2015. Disponível em <https://periodicos.uninove.br/prisma/article/viewFile/6304/3086>. Acesso em 19/03/2021.

MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (coord.). **LGPD: Lei Geral de Proteção de Dados: comentada**. 2. ed. rev. atual. e ampl. São Paulo: Revista dos Tribunais, 2019. 574 p.

MENDES, Laura Schertel. **Transparência e Privacidade: Violação e Proteção da Informação Pessoal na Sociedade de Consumo**. Brasília, 2008.

MOTA, Ivan Dias da; TENA, Lucimara Plaza. **Fundamentos da LGPD: círculos concêntricos e sociedade de informação no contexto de direitos da personalidade**. Revista Juridica, [S.l.], v. 2, n. 59, p. 538 - 576, set. 2020. ISSN 2316-753X. Disponível em: <http://revista.unicuritiba.edu.br/index.php/RevJur/article/view/4330>. Acesso em: 01/04/2021.

NABAIS, José Casalta. **O dever fundamental de pagar impostos**. Coimbra: Almedina. 4ª reimpressão, 2015.

PAULSEN, Leandro. **Curso de direito tributário completo**. 11. ed. São Paulo: Saraiva Educação, 2020. 999 p. E-book.

PINHEIRO, Patricia Peck. **Proteção de dados pessoais: comentários à Lei n. 13.709/2018 (LGPD)**. 2ª ed. São Paulo: Saraiva Educação, 2020. 152 p.

POLONI, Brayan. **O que é governança de dados?** 23/09/2019. Disponível em < https://introduceti.com.br/blog/o-que-e-governanca-de-dados/ >. Acesso em 31/03/2021.

RUARO, Regina Linden; RODRIGUES, Daniel Piñeiro; FINGER, Brunise. **O direito à proteção de dados pessoais e a privacidade.** Revista da Faculdade de Direito – UFPR, Curitiba, n. 58, 2011. Disponível em: < https://revistas.ufpr.br/direito/article/view/30768/19876 >. Acesso em: 31/03/2021.

SARDENBERG, Rodrigo de Castro. **Réquiem do sigilo bancário?** Disponível em: [www.jota.info/opiniao-e-analise/artigos/requiem-do-sigilo-bancario-27122019]. Acesso em: 23/03/2021.

SCHNEIDER, Rosane. **A (in)constitucionalidade da quebra do sigilo fiscal**. Disponível em: https://egov.ufsc.br/portal/conteudo/inconstitucionalidade-da-quebra-do-sigilo-fiscal-0. Acesso em 23/03/2021.

STF. **RE 1055941**. Disponível em: http://portal.stf.jus.br/processos/detalhe.asp?incidente=5213056. Acesso em 23/03/2021.

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. 2. ed. rev. atual. e ampl. São Paulo: Revista dos Tribunais, 2019. 574 p.

TEFFÉ, C. S. DE; VIOLA, M. **Tratamento de dados pessoais na LGPD: estudo sobre as bases legais**. civilistica.com, v. 9, n. 1, p. 1-38, 09/05/2020. Disponível em: < https://civilistica.emnuvens.com.br/redc/article/view/510/384 >. Acesso em 01/04/2021.

VAINZOF, Rony. **Capítulo I – Disposições Preliminares**. In: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (coord.). **LGPD: Lei Geral de Proteção de Dados: comentada**. 2. ed. rev. atual. e ampl. São Paulo: Revista dos Tribunais, 2019. 574 p.

WARREN, Samuel Dennis, BRANDEIS, Louis Dembitz. **The Right to Privacy.** Harvard Law Review. Volume IV, 15 de dezembro de 1890. Disponível em: <https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf>. Acesso em 25/02/2021.

UNIÃO EUROPEIA. **Convenção 108**, de 28 de janeiro de 1981. <https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680078b37>. Acesso em 24/02/2021.

_____. **Diretiva 95/46/CE**, de 23 de novembro de 1995. <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:31995L0046&from=PT>. Acesso em 24/02/2021.

_____. **Protecção de dados pessoais**. <https://eur-lex.europa.eu/legal-content/PT/LSU/?uri=CELEX:31995L0046>. Acesso em 24/02/2021.

_____. Regulamento (EU) 2016/679 do Parlamento e do Conselho Europeu, de 27 de abril de 2016. **General Data Protection Regulation.** Disponível em <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679>. Acesso em 22/02/2021.

ZANINI, Leonardo Estevam de Assis. **O surgimento e o desenvolvimento do *right of privacy* nos Estados Unidos**. Revista de Doutrina da 4ª Região, Porto Alegre, n.64, fev. 2015. Disponível em: <https://revistadoutrina.trf4.jus.br/artigos/edicao064/Leonardo_Zanini.html> Acesso em: 31/03/2021.