REPATS - Revista de Estudos e Pesquisas Avançadas do Terceiro Setor

REPATS, Brasília, V. 5, nº 2, p 157-187, Jul-Dez, 2018

A ANONIMIZAÇÃO DOS DADOS COMO FORMA DE RELATIVIZAÇÃO DA PROTEÇÃO DE INFORMAÇÕES SIGILOSAS E A ATUAÇÃO FISCALIZATÓRIA DOS TRIBUNAIS DE CONTAS

THE DATA ANONIMATION AS A WAY TO RELAX OF THE PROTECTION OF SECONDARY INFORMATION AND THE AUDIT OF THE COURT OF AUDIT

Fernando Simões dos Reis[*]
Regina Linden Ruaro [**]

RESUMO: Neste estudo, discute-se a possibilidade de relativização do direito fundamental à proteção de dados pessoais, mais especificamente o direito ao sigilo fiscal, frente ao dever fundamental dos tribunais de contas de exercer a sua atribuição fiscalizatória. Apresenta-se a evolução do direito à proteção de dados no tocante à possibilidade de tratamento de informações pelos órgãos estatais. Por meio de estudo de direito comparado, demonstra-se a possibilidade de utilização da técnica de anonimização de dados como solução nos casos de conflito entre a privacidade das informações e o interesse público de manipulação dos dados. Por fim, apresenta-se uma decisão do Tribunal de Contas da União em que já foi utilizada essa solução para que fosse possível a fiscalização de sistema da Receita Federal sem ofensa ao direito fundamental ao sigilo fiscal.
Palavras-chave: tribunal de contas; direitos fundamentais; proteção de dados; anonimização de dados; direito comparado.

ABSTRACT: *In this study, the possibility of relativizing the fundamental right to the protection of personal data, specifically the right to fiscal confidentiality, is discussed, in view of the fundamental duty of the courts of law to exercise their audit attribution. It presents the evolution of the right to data protection regarding the possibility of information processing by governmental entities. Analysing comparative law, the possibility of using the data anonymization technique is demonstrated as a solution in cases of conflict between the information privacy and the public interest in data manipulation. Finally, a decision is presented by the Federal Court of Auditors where this solution has already been used to make it possible to inspect a system of the Department of Federal Revenue (RFB) without offending the fundamental right to fiscal confidentiality.*

Recebido em: 12/08/2018
Aceito em: 19/08/2018

[*]Auditor Federal de Controle Externo do Tribunal de Contas da União. Mestrando em Direito pela Pontifícia Universidade Católica do Rio Grande do Sul. Bacharel em Ciências Jurídicas e Sociais pela Universidade Federal do Rio Grande do Sul.
[**]Doutora em Direito pela Universidad Complutense de Madrid – Espanha. Professora Titular da Faculdade de Direito da Pontifícia Universidade Católica do Rio Grande do Sul. Lidera o Grupo de Pesquisa Proteção de Dados Pessoais e Direito Fundamental de Acesso à Informação.

Keywords: *court of audit; fundamental rights, data protection; data anonymization; comparative law*

INTRODUÇÃO

Os órgãos de controle, na sua função precípua de fiscalização da atuação da Administração Pública, vêm cada vez mais necessitando de informações diante da necessidade de avaliação dos sistemas de informática utilizados para a gestão pública. Para uma avaliação adequada da eficácia desses sistemas, muitas vezes torna-se necessário o acesso a bancos de dados sigilosos que, em princípio, não podem ser objeto de compartilhamento pelos órgãos detentores da informação.

Neste estudo, discutir-se-á a relativização do direito fundamental à proteção de dados pessoais sobretudo dos que gozam de sigilo fiscal. Para atingir este objetivo, inicialmente, será exposta a evolução do direito à proteção de dados no tocante à possibilidade de tratamento de informações pelos órgãos estatais.

Também se analisará o conteúdo do direito ao sigilo fiscal por ser o mesmo decorrente do direito fundamental à proteção de dados e a possibilidade de sua relativização quando houver interesse público envolvido no tratamento das informações.

Na sequência, por meio de estudo do direito comparado, demonstrar-se-á que a técnica de anonimização dos dados é uma solução que pode ser adotada no direito nacional para possibilitar o compartilhamento das informações. Também será detalhado que essa técnica é adequada principalmente nos casos de conflito entre a privacidade das informações e o interesse público de manipulação dos dados.

Por fim, será trazido um Acórdão em que o Tribunal de Contas da União, ao solicitar informações do sistema da Receita Federal, sugeriu a esse órgão que os dados fossem anonimizados para que fosse possível a fiscalização do sistema sem ofensa ao direito fundamental ao sigilo fiscal. A par disto, também será discutida a adequação da medida da Corte Federal de Contas levando-se em conta o postulado da proporcionalidade.

O presente artigo é resultado de pesquisa do Grupo “A proteção de dados pessoais no Estado democrático de direito” e está alinhado à Linha de

pesquisa “Direito, Tecnologia e Inovação, do Programa de Pós-Graduação em Direito, da Escola de Direito da PUC-RS.

1. A PROTEÇÃO DE DADOS FRENTE AOS ÓRGÃOS ESTATAIS

A origem do à direito proteção de dados remonta ao final do Século XIX, quando começaram a aparecer novas tecnologias capazes de expor a vida privada das pessoas, ou seja, tem ligação ao aparecimento do direito à privacidade. O marco fundador desse direito é o famoso artigo de Samuel Warren e Louis Brandeis “*The right to privacy”*, onde os autores defendiam o direito de ser deixado só (*the right to be let alone*) diante do surgimento de novas invenções e métodos de negócio.[1] (WARREN, BRANDEIS, 1890)

Uma das grandes virtudes dessa obra de Warren e Brandeis é que, na lição de Victor Miranda (2016, p. 100-101), foi a primeira a perceber a necessidade dessa proteção com fundamento no direito à inviolabilidade da personalidade, ao contrário dos estudos anteriores que invocavam o direito de propriedade como fundamento contra a invasão da vida privada. Essa autonomia da privacidade em relação ao direito de propriedade acabou sendo confirmada posteriormente pela Suprema Corte norte-americana em diversas decisões.[2]

Ao longo do Século XX, com o forte progresso tecnológico que possibilitava cada vez mais a utilização de tecnologias capazes de obter dados dos indivíduos e a consequente violação do direito à privacidade, houve o aumento do debate acerca do tema. Em especial, destaca-se a evolução do

[1] Nesse estudo, esses autores citam o perigo das novas máquinas fotográficas portáteis, que possibilitavam o registro de situações da vida pessoal e a posterior publicação em jornais de grande circulação, pois a introdução de novas técnicas de impressão a um custo acessível facilitaria sobremaneira essa divulgação. No artigo, também se afirma a insuficiência das legislações da época, como as leis protetoras contra a injúria e a difamação para esse novo problema. (WARREN, BRANDEIS, 1890)

[2] Conforme Ana Maria Navarro e Gabriela Leonardos, a decisão pioneira de uma norte-americana que reconheceu o direito à privacidade de forma independente ao direito de propriedade foi o *leading case Pavesich v. New England Life Insurance Company.* Nessa decisão, a Suprema Corte do estado da Geórgia proibiu o uso público e sem consentimento de imagem pessoal. NAVARRO, Ana Maria e LEONARDOS, Gabriela. Privacidade Informacional: origem e fundamentos no Direito Norte-Americano. In: CONPEDI/UFF. (Org.). XXI Congresso Nacional do CONPEDI/UFF. 1ed.: FUNJAB, 2012, p. 305

direito europeu. A Convenção Europeia dos Direitos do Homem, de 1950, já assegurava o respeito à vida privada familiar em seu artigo 8º[3]. Entretanto, a proteção de dados como direito fundamental expressamente autônomo foi positivado apenas na Carta dos Direitos Fundamentais da União Europeia, do ano 2000.

Ainda que não haja previsão expressa no nosso texto constitucional do direito à proteção de dados, Ingo Sarlet o considera como direito fundamental que está associado ao direito à privacidade, previsto no artigo 5ª, inciso X, da Constituição Federal, e ao direito ao livre desenvolvimento da personalidade, que inclui o direito à livre disposição dos dados pessoais. (SARLET; MARINONI; MITIDIERO, 2016, p. 469)

A Constituição Federal brasileira não concebeu, expressamente, um direito geral de personalidade. No entanto, o princípio constitucional da dignidade da pessoa humana é o postulado assecuratório da tutela da personalidade e dos consectários atribuídos nela investidos. Na lição de Ingo Sarlet, a ligação do direito à privacidade com a dignidade da pessoa humana se justifica na medida em que a preservação de uma esfera da vida privada é essencial à própria saúde mental do ser humano, lhe assegurando o pleno desenvolvimento de sua personalidade. (SARLET; MARINONI; MITIDIERO, 2016, p. 443)

Até pouco tempo atrás, a utilização dos dados pessoais de forma sistemática era basicamente feita pelo Estado, que, diante do alto custo da tecnologia, era o único ente capaz de coletar, por meio de censos e pesquisas, e gerenciar as informações. Recentemente, com o grande desenvolvimento tecnológico, especialmente com o avanço da informática nas últimas décadas, o acesso e o tratamento de informações têm sido feitos também por

[3] Artigo 8º
Protecção de dados pessoais
1. Todas as pessoas têm direito à protecção dos dados de carácter pessoal que lhes digam respeito.
2. Esses dados devem ser objecto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respectiva rectificação. (UNIÃO EUROPEIA, 2000)

organismos particulares, o que levou à necessidade de discutir o direito à proteção de dados em relação à atuação de entidades privadas.[4]

A justificativa para o acesso do Estado aos dados pessoais repousa no pressuposto que a administração pública eficiente é aquela que tem profundo conhecimento das características da população, o que justificaria, inclusive, em certas situações, o estabelecimento de regras compulsórias para a comunicação de determinadas informações aos órgãos estatais. (DONEDA 2006, p. 13-14). Essa necessidade de controle destinada a aumentar a eficiência, se por vezes é absolutamente necessária, outras, acaba colidindo com o direito à privacidade dos cidadãos. A consequência desta realidade gera litígios que irão desaguar no Poder Judiciário. Como exemplos, cabe trazer algumas decisões históricas no direito comparado que discutiram essa controvérsia.

Examinando o direito norte-americano, encontram-se duas decisões paradigmáticas da Suprema Corte de 1967 – *Berger v. New York* e *Katz v. United States* – que consideraram ilegal a coleta pelo Estado de informações pessoais obtidas por meio de escutas telefônicas sem o devido conhecimento e consentimento das pessoas afetadas ou prévia autorização judicial. Nessa segunda decisão, observou-se que, mesmo que as conversações fossem mantidas em cabines telefônicas públicas, a situação de ilegalidade permanecia. Para justificar essa decisão, a Suprema Corte formulou o conceito da "expectativa razoável de privacidade"[5], conforme sugestão do *Justice* Harlan, para que fosse possível mensurar a existência da lesão nos casos concretos. (UNITED STATES, 1967 b)

[4] A discussão do tratamento de dados pessoais por entidades privadas não é objeto de discussão no presente estudo. No entanto, em face de sua importância entendeu-se por referir-lhe.

[5] No original em inglês, segue a afirmação do Justice Harlan: "*My understanding of the rule that has emerged from prior decisions is that there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as "reasonable." Thus, a man's home is, for most purposes, a place where he expects privacy, but objects, activities, or statements that he exposes to the "plain view" of outsiders are not "protected," because no intention to keep them to himself has been exhibited. On the other hand, conversations in the open would not be protected against being overheard, for the expectation of privacy under the circumstances would be unreasonable.*" (UNITED STATES, 1967 b)

Nesse mesmo ano de 1967, Miguel Gayo chama a atenção para o estudo de Alan F. Westin, que se preocupou com os mecanismos de vigilância de chamadas telefônicas, os quais permitiam a fuga dos controles legais e sociais tradicionais de privacidade. Nesse estudo, este doutrinador colocou pela primeira vez como elemento integrante do direito à privacidade o direito dos indivíduos ou organizações determinarem por si mesmos quando e em qual medida as informações coletadas pelo poder público podem ser comunicadas a terceiros. (GAYO, 2016, p. 15)

Outro caso paradigmático ocorreu na Alemanha no início dos anos 80. Ainda que já existisse nesse país uma lei federal que regulasse a matéria de proteção de dados, ela se mostrou insuficiente para a proteção dos cidadãos quando o Estado, valendo-se de uma lei, pretendia finalizar um censo geral em 1983 com vistas a confrontar os dados fornecidos com os constantes do registro civil. Dentre os pontos que suscitaram controvérsia em relação a esse censo, citam-se os seguintes: existência de perguntas de cunho pessoal que abordavam desde aspirações profissionais dos indivíduos até suas práticas religiosas e políticas; possibilidade de transmissão dos dados recolhidos a outras autoridades e a possibilidade de aplicação de multa às pessoas que se negassem a responder as questões. (RUARO, RODRIGUEZ, p. 191)

Diante desses problemas, surgiu um sentimento generalizado de insegurança no país, pois se temia a criação de um Estado superinformado, o que resultou na discussão judicial da matéria. O processo terminou com o pronunciamento da Corte Constitucional Alemã, que terminou por julgar inconstitucional a lei sob o argumento de que os dados recolhidos poderiam ser utilizados para fins tanto administrativos como estatísticos, o que impediria o cidadão de saber exatamente qual era a finalidade do uso das informações. Além disso, entendeu-se que não era razoável que o rigor estatístico justificasse a necessidade dos órgãos administrativos identificar os titulares dos dados.[6] (RUARO, RODRIGUEZ, p. 191)

[6] Na lição de Danilo Doneda (2006, p. 196), essa sentença da Corte Constitucional Alemã que julgou inconstitucional a lei do censo acabou por consagrar a ideia de autodeterminação informativa, que se trata do direito dos indivíduos “de decidirem por si próprios, quando e dentro de quais limites seus dados pessoais podem ser utilizados”. Esse novo conceito é tão importante que Stefano Rodotà o considera o fim da linha do processo evolutivo experimentado

Pelo visto nessas decisões, a proteção de dados dos cidadãos está em constante conflito com a necessidade dos governos de obter informações para uma administração mais eficiente, que também é do interesse da coletividade. Assim, eventual restrição ao direito à proteção de dados vai se justificar pelo menor ou maior grau de sensibilidade das informações que pode afetar o núcleo da esfera pessoal do indivíduo bem como pelo grau de necessidade de informações para que o Estado possa exercer suas competências.[7]

2. O SIGILO FISCAL E SUA RELATIVIZAÇÃO FRENTE À NECESSIDADE DE CONTROLE DA ADMINISTRAÇÃO PÚBLICA

Primeiramente cabe referir que a exemplo do que ocorre com o direito à proteção de dados pessoais, também o direito ao sigilo fiscal não está, expressamente, previsto na Constituição Federal brasileira. No entanto, entende-se que este deriva do direito fundamental à proteção de dados, decorrente do artigo 5º, incisos X e XII. Ingo Sarlet aponta que a doutrina e a jurisprudência no Brasil vêm assim entendendo, ainda que esse autor reconheça que se trata de uma dimensão mais fraca da proteção à vida privada, diante da amplitude de situações em que é aceita a intervenção nesse direito, o que coloca em dúvida inclusive a sua condição de direito fundamental.[8] (SARLET; MARINONI; MITIDIERO, 2016, p. 449)

Reconhecendo-se, porém, o sigilo fiscal como verdadeiro direito fundamental decorrente do direito à proteção dos dados, conforme posicionamento de nossa Suprema Corte, deve ser melhor discutido em que hipóteses essa proteção poderia ser relativizada levando-se em conta a

pelo conceito de privacidade até uma ideia de efetiva proteção dos dados. (RODOTÀ, 2008, p. 17)

[7] Em relação a isso, Laura Mendes afirma que a proteção excessiva dos dados pode inclusive vir a impedir indevidamente que a Administração Pública venha a exercer suas atribuições. (MENDES, 2011, p. 46)

[8] Independente dessa controvérsia, o STF vem reconhecendo a necessidade de autorização judicial para a quebra desse sigilo, conforme previsto no artigo 198, §1º, inciso I do Código Tributário Nacional (CTN), dispensando apenas nos seguintes casos: quando a quebra do sigilo for requisitada por comissão parlamentar de inquérito para investigação, sendo que o pedido deve estar devidamente motivado[8] ou quando requisitada por autoridade fiscal, nos termos da Lei Complementar n. 105/2018.

possibilidade de conflito com outros direitos fundamentais ou interesses da coletividade.

Primeiramente, deve-se ressaltar que, ainda que os direitos fundamentais tenham um âmbito de proteção privilegiado em relação a outros direitos, eles não são absolutos. Na formulação de sua teoria dos direitos fundamentais, Robert Alexy argumenta contra a inexistência de princípios absolutos, nos seguintes termos:

> É fácil argumentar contra a existência de princípios absolutos em um ordenamento jurídico que inclua direitos fundamentais. Princípios podem se referir a interesses coletivos ou a direitos individuais. Se um princípio se refere a interesses coletivos e é absoluto, as normas de direitos fundamentais não podem estabelecer limites jurídicos a ele. Assim, até onde o princípio absoluto garante direitos individuais, a ausência de limites desse princípio levaria à seguinte situação contraditória: em caso de colisão, os direitos de cada indivíduo, fundamentados pelo princípio absoluto, teriam que ceder em favor dos direitos de todos os indivíduos, também fundamentados pelo princípio absoluto. Diante disso, ou os princípios absolutos não são compatíveis com direitos individuais, ou os direitos individuais que sejam fundamentados pelos princípios absolutos não podem ser garantidos a mais de um sujeito de direito. (ALEXY, 2011, p. 111)

Ignacio de Otto y Pardo é outro autor que defende a limitação dos direitos fundamentais. Ao tratar dos limites imanentes dos direitos fundamentais, esse doutrinador defende a necessária existência de uma conciliação de um com os demais nos seguintes termos:

> Los derechos fundamentales no están sometidos únicamente a lós limites que de manera expresa lês imponen las normas constitucionales que lós reconocen, sino también a lós que resulten justificadas por La protección de lós derechos y bienes a que se alude, esto es, están sujetos a uma limitación genérica establecida de modo tácito para todo derecho.[9]

Por seu lado, Ingo Sarlet ao estudar a proteção dos direitos fundamentais salienta que

> a ideia de que os direitos fundamentais não são absolutos, no sentido de absolutamente blindados contra qualquer tipo de restrição na sua esfera subjetiva e objetiva, não tem oferecido maiores dificuldades,

[9] OTTO Y PARDO, Ignacio de. **La Regulación del ejercício de lós derechos y Libertades.** Madrid:Cuadernos Civitas. 1988. p. 110.

> tendo sido, de resto, amplamente aceita no direito constitucional contemporâneo[10]

Efetivamente, não se pode pretender e, sequer seria factível, que todos os direitos fundamentais tivessem um caráter absoluto e isto porque com tal premissa, dentre outros fatores, para o objeto do estudo aqui realizado, em eventual colisão entre um e outro, se estaria diante de um problema jurídico sem solução. É imperativo ao sistema jurídico apresentar soluções que sejam capazes de resolver colisões de direitos.

Segundo Sarlet (2015, p. 410-411), a relativização desses direitos pode ocorrer nas seguintes hipóteses: expressa disposição constitucional; existência de norma legal promulgada com fundamento na Constituição e por força de conflitos entre direitos fundamentais, no caso daqueles formalmente ilimitados, situação em que deverá se realizar a devida ponderação.

Ante a inexistência de expressa disposição constitucional que limite o acesso aos dados sob sigilo fiscal, recorre-se às possibilidades de relativização desse direito dispostas nas normas infraconstitucionais. A limitação, no caso do sigilo fiscal, seria dada pelo que está definido no artigo 198 do CTN, que veda a divulgação dos dados fiscais dos contribuintes pelas autoridades fiscais, podendo ser divulgadas as informações apenas no caso de requisição judicial ou quando houver solicitação de autoridade administrativa para investigação do sujeito passivo por prática de infração administrativa.[11]

Importante ressaltar que, da mesma forma que o dispositivo mencionado do CTN dispõe sobre o direito fundamental ao sigilo fiscal, a Lei n. 8.443/1992 (Lei Orgânica do TCU) regulamenta outro princípio constitucional de sujeição dos órgãos da Administração Pública ao controle externo, inclusive

---

[10] SARLET, Ingo Wolfgang. **A eficácia dos direitos fundamentais.** 12ª ed. Porto Alegre: Livraria do Advogado. 2015. p .405-406.

[11] Segue transcrição do mencionado comando do CTN:
Art. 198. Sem prejuízo do disposto na legislação criminal, é vedada a divulgação, por parte da Fazenda Pública ou de seus servidores, de informação obtida em razão do ofício sobre a situação econômica ou financeira do sujeito passivo ou de terceiros e sobre a natureza e o estado de seus negócios ou atividades.
§ 1º Excetuam-se do disposto neste artigo, além dos casos previstos no art. 199, os seguintes:
I – requisição de autoridade judiciária no interesse da justiça;
II – solicitações de autoridade administrativa no interesse da Administração Pública, desde que seja comprovada a instauração regular de processo administrativo, no órgão ou na entidade respectiva, com o objetivo de investigar o sujeito passivo a que se refere a informação, por prática de infração administrativa.

o responsável pela arrecadação dos tributos, conforme os artigos 70 e 71 da Constituição Federal. De acordo com o artigo 1º, inciso IV, dessa Lei, compete ao Tribunal de Contas da União, órgão que exerce o controle externo em auxílio ao Congresso Nacional, acompanhar a arrecadação da receita a cargo da União mediante fiscalizações.[12] Evidentemente, para o exercício dessa competência, uma das formas que a Corte Federal de Contas possui é o acesso aos sistemas das autoridades responsáveis pela arrecadação, sendo que esses bancos de dados podem conter informações protegidas pelo sigilo fiscal.

Em busca de normas legais que regulamentem a matéria, há duas normas que colidem entre si: o CTN, que dispõe sobre o direito fundamental ao sigilo fiscal, trazendo a vedação da divulgação dos dados fiscais dos contribuintes, e a Lei n. 8.443/1993, que traz a obrigação do TCU de acompanhar a arrecadação da receita, vindo ao encontro do interesse coletivo de uma Administração Pública mais eficiente. Ressalta-se que inexiste norma específica que trate da forma que as autoridades fiscais devem fornecer os dados para o exercício das competências fiscalizatórias dos tribunais de contas.

Portanto, essa controvérsia deve ser solucionada pela ponderação entre princípios, pois o que se vê aqui é a colisão de direitos fundamentais que deverão ser objeto de relativização com vistas a que o núcleo essencial de ambos não seja atingido. Nem o interesse da sociedade da devida fiscalização dos órgãos públicos pode ser prejudicado em sua essência, nem o direito à privacidade – nesse caso traduzido no sigilo dos dados fiscais – pode ser objeto de total desconsideração. É necessário achar alguma alternativa que possibilite a preservação dessas garantias constitucionais, pois não se pode falar que um princípio deve preponderar sobre o outro antes da análise do caso concreto. Deve se tentar ao máximo a preservação do sistema como um todo,

[12] Segue transcrição do mencionado comando da Lei n. 8.443/1992:
Art. 1° Ao Tribunal de Contas da União, órgão de controle externo, compete, nos termos da Constituição Federal e na forma estabelecida nesta Lei:
IV - acompanhar a arrecadação da receita a cargo da União e das entidades referidas no inciso I deste artigo, mediante inspeções e auditorias, ou por meio de demonstrativos próprios, na forma estabelecida no Regimento Interno;

vindo ao encontro de uma interpretação sistemática do direito, conforme bem leciona Juarez Freitas.[13] (FREITAS, 2010, p. 214)

3. A ANONIMIZAÇÃO DOS DADOS COMO SOLUÇÃO DA CONTROVÉRSIA

Conforme exposto, diante da inexistência de legislação infraconstitucional no Brasil que regulamente a manipulação de informações sigilosas pelas cortes de contas, deve-se buscar uma solução que possa preservar o núcleo de ambos os direitos fundamentais mencionados. No caso da proteção de dados, entende-se pertinente buscar a solução por analogia no direito europeu, que reconhecidamente já avançou bastante em termos de regulamentação da matéria. A seguir, mostrar-se-á a evolução da legislação europeia em termos de proteção de dados pessoais e de como se chegou à conclusão que a anonimização das informações pode ser uma boa solução em caso de conflito entre direitos envolvendo a privacidade dos dados.

Como já mencionado, da mesma forma que o artigo 5º, inciso X, da nossa Constituição Federal, a Convenção Europeia dos Direitos do Homem, de 1950, já assegurava o respeito à vida privada familiar em seu artigo 8º, nos seguintes termos:

> Artigo 8º
> 1. Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência.
> 2. Não pode haver ingerência de autoridade pública no exercício deste direito senão quando esta ingerência estiver prevista na lei e constituir uma providência que, numa sociedade democrática, seja necessária para a segurança nacional, para a segurança pública, para o bem-estar econômico do país, a defesa da ordem e a prevenção das infracções penais, a protecção da saúde ou da moral, ou a protecção dos direitos e das liberdades de terceiros. (UNIÃO EUROPEIA, 1950).

[13] Acerca da inexistência da preponderância de princípios fundamentais em abstrato, cabe trazer trecho da obra do referido administrativista: “A rigor, inexiste direito fundamental dotado da apriorística primazia cabal e solitária, dada a intersubjetividade dos direitos, de maneira que sequer a dignidade pode ser vista como absoluta, uma vez que o respeito à dignidade supõe proteção isonômica de todas as dignidades. Assim é que se deve interpretar a totalidade dos direitos fundamentais, no seio de nossa Constituição, isto é, de maneira proporcional, como o resultado de mútua e salutar relativização. Não enfraquece, mas, ao contrário, fortalece a totalidade dos princípios, objetivos e direitos fundamentais o fato de serem reciprocamente complementares.” (FREITAS, 2010, p. 214)

Pela leitura dos dois dispositivos citados, existe a clara ideia que esse direito não é absoluto. Já na Convenção de 1950, foram trazidas algumas possibilidades de ingerência pela autoridade pública justificadas basicamente pelo interesse público ou para a proteção de direitos e liberdades de outros indivíduos. Posteriormente, a Carta de Direitos Fundamentais da União Europeia, editada em 2000, veio a confirmar a relativização da proteção de dados, trazendo como hipóteses para isso o consentimento da pessoa ou outro fundamento previsto em lei.

Ainda com base no mencionado artigo da Convenção Europeia dos Direitos do Homem, foram editados alguns normativos acerca da proteção de dados pessoais. Dentre eles, destaca-se sobremaneira a Convenção para a Proteção das Pessoas relativamente ao Processamento Automático de Dados Pessoais, de 1981 (Convenção 108/1981), que foi o primeiro instrumento jurídico internacional vinculativo nesse domínio. Essa normativa aplicava-se a todos os tratamentos de dados pessoais realizados pelo setor público e pelo setor privado, inclusive sobre os tratamentos de dados efetuados por autoridades governamentais.

A Convenção n. 108/1981 destaca-se no que diz respeito às balizas principiológicas que ela trouxe para harmonizar a necessidade de compartilhamento de dados pessoais sem suprimir a essência do direito à proteção de dados. Dentre os princípios que se pode extrair dessa norma, destacam-se os seguintes:[14]

1) Princípio da especificação e da limitação da finalidade (artigo 5º, alínea b, da Convenção 108/1981): o propósito ao qual se destina a obtenção de dados deve ser delimitado, não se admitindo a obtenção e o armazenamento para fins indefinidos;

2) Princípio do tratamento lícito (artigo 5º, alíneas a e b, da Convenção 108/1981): os dados devem ser obtidos e tratados para os fins especificados

[14]Esses princípios estão detalhadamente explicados no Manual da legislação europeia de proteção de dados. Disponível em <file:///C:/Users/Fernando/Downloads/fra-2014-handbook-data-protection-pt.pdf>. Acesso em 2 de junho de 2017.

legalmente, sendo proibida a utilização das informações para propósitos diversos da previsão legal;

3) Princípio da limitação da conservação dos dados (artigo 5º, alínea e, da Convenção 108/1981): o armazenamento dos dados não pode ser indefinido, devendo se limitar ao tempo estritamente necessário ao alcance do propósito para o qual foi feita a coleta;

4) Princípio do tratamento leal (artigo 5º, alínea a, da Convenção 108/1981): o tratamento dos dados deve ser transparente, sendo proibido o tratamento secreto salvo nos casos expressamente previstos em lei.

Além disso, durante o tratamento dos dados, o artigo 15, item 2, da Convenção 108/1981 exige que as autoridades designadas que tenham recebido os dados providenciem o adequado sigilo e confidencialidade dessas informações.

No entanto, é importante analisar também a definição que essa convenção traz para dados pessoais. Conforme o artigo 2º, o conceito de dados de caráter pessoal significa qualquer informação relativa a uma pessoa singular identificada ou suscetível de identificação, conforme tradução do original em inglês abaixo:

> *Article 2 – Definitions*
> *For the purposes of this Convention:*
> *a."personal data" means any information relating to an identified or identifiable individual ("data subject");*(UNIÃO EUROPEIA, 1981)

Essa definição não pode ser lida de forma isolada. Para entender o que significa uma pessoa suscetível de identificação, faz-se necessário uma remissão ao Relatório Explicativo que acompanha a referida Convenção. Segundo o item 28 desse relatório, o conceito de indivíduo identificável significa uma pessoa que pode ser facilmente identificada, não abrangendo a identificação de pessoas por meio de métodos muito sofisticados, conforme tradução do original em inglês a seguir: "*28. 'Identifiable persons' means a person who can be easily identified: it does not cover identification of persons by means of very sophisticated methods*". (UNIÃO EUROPEIA, 1981)

Portanto, já nessa regulamentação, havia a previsão da possibilidade de tratamento de dados pessoais identificáveis, desde que fossem devidamente mascarados de alguma maneira que não possibilitasse facilmente a identificação. Pela primeira vez, portanto, foi referenciada a técnica de anonimização, mesmo que de forma implícita, como forma de relativização do sigilo dos dados.

Após isso, a União Europeia adotou a Diretiva n. 46 do Parlamento Europeu e do Conselho, de 1995 (Diretiva 46/1995), relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Salienta-se que a diretiva é um ato legislativo editado para detalhar ou concretizar regras fundamentais previstas nos tratados, como é o caso da Convenção 108. Ainda, a diretiva tem caráter vinculativo, criando a obrigação de cada país confirmar sua legislação interna de acordo com os objetivos traçados nesse regulamento.

Essa nova normativa seguiu basicamente a mesma base principiológica da Convenção 108/1981. Além disso, trouxe, em seu artigo 7º, parâmetros para a legitimidade do tratamento de dados. Duas hipóteses para o referido tratamento é justamente o interesse público e a existência de uma obrigação prevista em lei, conforme alíneas c) e e) do referido comando normativo, abaixo transcritos:

> Artigo 7º
> Os Estados-membros estabelecerão que o tratamento de dados pessoais só poderá ser efectuado se:
> (...)
> c) O tratamento for necessário para cumprir uma obrigação legal à qual o responsável pelo tratamento esteja sujeito; ou
> (...)
> e) O tratamento for necessário para a execução de uma missão de interesse público ou o exercício da autoridade pública de que é investido o responsável pelo tratamento ou um terceiro a quem os dados sejam comunicados; (UNIÃO EUROPEIA, 1995)

A possibilidade de um órgão de controle ter acesso a informações pessoais é reforçada no artigo 13 da Diretiva, que traz as possibilidades de restrição à proteção de dados, conforme item 1, alíneas d), e) e f), nos seguintes termos:

> Artigo 13 - Derrogações e restrições
> 1 . Os Estados-membros podem tomar medidas legislativas destinadas a restringir o alcance das obrigações e direitos referidos no nº 1 do artigo 6º no artigo 10º, no nº 1 do artigo 11 e nos artigos 12º e 21º, sempre que tal restrição constitua uma medida necessária à protecção:
> (...)
> d) Da prevenção, investigação, detecção e repressão de infracções penais e de violações da deontologia das profissões regulamentadas;
> e) De um interesse econômico ou financeiro importante de um Estado-membro ou da União Europeia, incluindo nos domínios monetário, orçamental ou fiscal;
> f) De missões de controlo, de inspecção ou de regulamentação associadas, ainda que ocasionalmente, ao exercício da autoridade pública, nos casos referidos nas alíneas c), d) e e); (UNIÃO EUROPEIA, 1995)

De imediato, é notória a semelhança do ordenamento europeu com a situação prevista em nossa Constituição Federal, já que o ordenamento europeu admite a limitação do tratamento de dados pessoais tanto para atender as necessidades financeiras do estado, em consonância com o artigo 145, §1º, da Magna Carta, bem como para permitir inspeções ou missões de controle por autoridades públicas, o que vem ao encontro do artigo 70, parágrafo único, da Constituição Federal.

Outro comando que é fundamental ser citado da Diretiva é o artigo 17, que trata da segurança do tratamento dos dados. Nesse dispositivo, é dito que devem ser colocadas em práticas medidas técnicas adequadas para a proteção dos dados pessoais contra eventuais tratamentos ilícitos. No entanto, exige-se dessas medidas “um nível de segurança adequado em relação aos riscos que o tratamento apresenta e à natureza dos dados a proteger”. (UNIÃO EUROPEIA, 1995) Em outras palavras, a própria diretiva aceita o fato que não se pode exigir uma segurança absoluta, sob pena de impossibilitar o tratamento de dados naqueles casos considerados fundamentais.

Vindo ao encontro desse raciocínio de proteção adequada dos dados, o Considerando 26 da Diretiva, pela primeira vez no ordenamento europeu, admitiu a técnica de anonimização como uma solução razoável que pode ser adotada, de acordo com a transcrição abaixo:

> (26) Considerando que os princípios da protecção devem aplicar-se a qualquer informação relativa a uma pessoa identificada ou identificável ; que, para determinar se uma pessoa é identificável,

> importa considerar o conjunto dos meios susceptíveis de serem razoavelmente utilizados, seja pelo responsável pelo tratamento, seja por qualquer outra pessoa, para identificar a referida pessoa; que os princípios da protecção não se aplicam a dados tornados anônimos de modo tal que a pessoa já não possa ser identificável ; que os códigos de conduta na acepção do artigo 27º podem ser um instrumento útil para fornecer indicações sobre os meios através dos quais os dados podem ser tornados anônimos e conservados sob uma forma que já não permita a identificação da pessoa em causa; (UNIÃO EUROPEIA, 1995)

Após a edição da Carta de Direitos Fundamentais da União Europeia, em 2000, na qual foi expressamente reconhecida a proteção de dados como direito fundamental autônomo, intensificaram-se os esforços para uma melhor regulamentação da questão no continente europeu. A grande evolução tecnológica nas áreas de coleta, manipulação e tratamento de dados abriu amplas possibilidades para a violação do direito à proteção dos dados, gerando a necessidade de uma legislação mais completa. Nesse sentido, foi editado o Regulamento 2016/679 do Parlamento Europeu e do Conselho, em 27 de abril de 2016, que substituiu a Diretiva 46/1995.[15]

Em suma, esse novo regulamento veio a confirmar as ideias expostas aqui sobre o tratamento de dados por autoridades governamentais, conforme abaixo exposto (UNIÃO EUROPEIA, 2016):

1) A base principiológica relativa ao tratamento de dados pessoais, estabelecida primeiramente na Convenção 108/1981, foi mantida, de acordo com o disposto no artigo 5º;

2) O tratamento dos dados por órgãos governamentais se manteve como prática lícita, desde que em cumprimento de uma obrigação legal ou se a manipulação dos dados for realizada no exercício de funções de interesse público, conforme disposto no artigo 6º, item 1, alíneas c) e e), e item 2;

3) A possibilidade dos Estados-membros tomarem medidas legislativas com vistas a limitar o direito à proteção de dados se manteve nos casos de interesse público geral, notadamente nos domínios monetário, orçamentário ou fiscal, e em situações de missões de controle e de inspeção por autoridades

[15] Conforme o artigo 99, o regulamento já entrou em vigor, mas somente será aplicável a partir de 25 de maio de 2018. Disponível em: <http://eur-lex.europa.eu/legal-content/pt/TXT/PDF/?uri=CELEX:32016R0679&from=EN>. Acesso em 30 de maio de 2017.

públicas no exercício de suas competências, com fulcro no artigo 23, item 1, alíneas e) e h);

4) Quanto à segurança do tratamento de dados, foi mantida a ideia de existência de um nível adequado de segurança relativamente aos riscos, fugindo-se da ideia de uma segurança absoluta, conforme o artigo 32;

5) Por fim, a definição de dados pessoais manteve a mesma ideia de informação acerca de um indivíduo identificada ou ao menos identificável. Ainda, da mesma forma que na Diretiva 46/1995, na seção de considerandos, foi feita a seguinte observação a respeito do que deve ser considerada uma pessoa identificável:

> (26) Os princípios da proteção de dados deverão aplicar-se a qualquer informação relativa a uma pessoa singular identificada ou identificável. Os dados pessoais que tenham sido pseudonimizados, que possam ser atribuídos a uma pessoa singular mediante a utilização de informações suplementares, deverão ser considerados informações sobre uma pessoa singular identificável. Para determinar se uma pessoa singular é identificável, importa considerar todos os meios suscetíveis de ser razoavelmente utilizados, tais como a seleção, quer pelo responsável pelo tratamento quer por outra pessoa, para identificar direta ou indiretamente a pessoa singular. Para determinar se há uma probabilidade razoável de os meios serem utilizados para identificar a pessoa singular, importa considerar todos os fatores objetivos, como os custos e o tempo necessário para a identificação, tendo em conta a tecnologia disponível à data do tratamento dos dados e a evolução tecnológica. Os princípios da proteção de dados não deverão, pois, aplicar-se às informações anônimas, ou seja, às informações que não digam respeito a uma pessoa singular identificada ou identificável nem a dados pessoais tornados de tal modo anônimos que o seu titular não seja ou já não possa ser identificado. O presente regulamento não diz, por isso, respeito ao tratamento dessas informações anônimas, inclusive para fins estatísticos ou de investigação. (UNIÃO EUROPEIA, 2016)

Ante o exposto, no novo regulamento, manteve-se a ideia de possibilidade de tratamento de dados anonimizados como forma razoável de relativização do direito à proteção dos dados, desde que a técnica utilizada torne a reidentificação das informações do titular bastante improvável, diante do nível de evolução tecnológica disponível à época da manipulação dos dados.

No que diz respeito à possibilidade de se adotar a experiência do direito estrangeiro, como já mencionado anteriormente, não existe legislação

no Brasil que regulamente o tratamento de dados sigilosos pelos órgãos de controle. Na falta de regulamentação específica no Brasil, a solução foi buscar no direito comparado, por analogia, alguma forma de possibilitar o acesso dos dados para que os órgãos de controle possam exercer suas competências constitucionais e legais sem comprometer o núcleo essencial do sigilo dos dados fiscais dos contribuintes. Vale lembrar que a própria Lei de Introdução às normas do Direito Brasileiro (Decreto-Lei n. 4.657/1942) traz essa possibilidade em seu artigo 4º: "Quando a lei for omissa, o juiz decidirá o caso de acordo com a analogia, os costumes e os princípios gerais de direito".[16]

A adequação dessa analogia é reforçada pelo texto do Projeto de Lei do Senado n. 330/2013 (PLS 330/2013), que visa a estabelecer princípios, garantias, direitos e obrigações referentes à proteção, ao tratamento e uso de dados pessoais. Esse projeto legislativo, em tramitação no Congresso Nacional, já acolhe o conceito consagrado internacionalmente de anonimização de dados, buscando internalizar experiência já vigente no direito comparado. Em seu artigo 3º, incisos XIII e XIV, são trazidas as seguintes definições:

> Artigo 3º Para os efeitos desta Lei, considera-se:
> XIII – dissociação ou anonimização: procedimento ou modificação destinado a impedir a associação de um dado pessoal a um indivíduo identificado ou identificável ou capaz de retirar dos dados coletados ou tratados as informações que possam levar à identificação dos titulares;
> XIV – dado anonimizado ou anônimo: dado relativo a um titular que não possa ser identificado, considerando a utilização dos meios técnicos razoáveis e disponíveis na ocasião de sua coleta ou tratamento. (BRASIL, Senado Federal, 2013)

A seguir, serão apresentados casos concretos de atuação do TCU nos quais foi debatida a questão de acesso à sistema da Secretaria da Receita Federal do Brasil (RFB) que continha informações protegidas pelo sigilo fiscal bem como a solução adotada pela Corte Federal de Contas para solução da controvérsia.

4. A UTILIZAÇÃO DA ANONIMIZAÇÃO DE DADOS PARA O ACESSO DE DADOS PELO TCU

[16]BRASIL. Decreto-Lei n. 4.657, de 4 de setembro de 1942. Planalto. Lei de Introdução às normas dos Direito Brasileiro. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/Del4657compilado.htm>. Acesso em 2 de junho de 2017.

Em 2007, o TCU, em cumprimento da competência de fiscalização prevista no artigo 1º, inciso IV, de sua Lei Orgânica, realizou auditoria na RFB com o objetivo de verificar os procedimentos de importação e exportação relacionados à sistemática aduaneira do Canal Verde.[17] Para alcançar os objetivos da fiscalização, foram solicitados à RFB acesso às informações registradas no Sistema Integrado de Comércio Exterior (Siscomex). No entanto, sob a alegação da existência de dados protegidos pelo sigilo fiscal, o órgão fiscal recusou o pleno acesso às informações registradas no sistema.

Em face dessa negativa, a equipe de auditoria formulou representação por sonegação de informações, com fulcro no art. 42 da Lei n. 8.443/1992[18], acolhida no Acórdão n. 1835/2007-TCU-Plenário, que terminou por fixar prazo para que titular da RFB apresentasse as informações requeridas, alertando-o inclusive pela possibilidade de aplicação de multa em caso de nova negativa, conforme previsto no artigo 58 da Lei 8.443/1992. (TCU, 2007)

Ocorre que o então Secretário da Receita Federal do Brasil impetrou o Mandado de Segurança n. 27.091 – Distrito Federal, junto ao Supremo Tribunal Federal, contra a determinação supramencionada, no âmbito do qual o Ministro Gilmar Mendes deferiu pedido de medida cautelar para suspendê-la.[19] Ressalta-se que, em 30/3/2017, o Pretório Excelso proferiu a decisão de mérito, relatada pelo Ministro Luís Roberto Barroso, concedendo a segurança ao impetrante e determinando a anulação do item do Acórdão referido que determinava à RFB o acesso às informações do Siscomex sob o argumento

[17] Essa auditoria foi realizada no âmbito do TCU por meio do processo administrativo TC 025.686/2006-7.

[18] Segue transcrição do mencionado comando da Lei n. 8.443/1992:
Art. 42. Nenhum processo, documento ou informação poderá ser sonegado ao Tribunal em suas inspeções ou auditorias, sob qualquer pretexto.
§ 1° No caso de sonegação, o Tribunal assinará prazo para apresentação dos documentos, informações e esclarecimentos julgados necessários, comunicando o fato ao Ministro de Estado supervisor da área ou à autoridade de nível hierárquico equivalente, para as medidas cabíveis.
§ 2° Vencido o prazo e não cumprida a exigência, o Tribunal aplicará as sanções previstas no inciso IV do art. 58 desta Lei.

[19] Essa medida liminar foi deferida em 4 de janeiro de 2008, conforme Despacho do Ministro Gilmar Mendes. Disponível em: <http://stf.jus.br/portal/processo/verProcessoTexto.asp?id=2278753&tipoApp=RTF>. Acesso em 2 de outubro de 2017.

que a concessão ampla e irrestrita de dados fiscais ínsitos à privacidade dos contribuintes, sem a devida ocultação de suas identidades, acarretaria violação ao direito fundamental à privacidade assegurado no artigo 5º, inciso X, da Constituição Federal. (STF, 2017)

Diante da concessão da liminar que impedia o acesso às informações do sistema da RFB pelo TCU e tendo em vista a necessidade do exercício de suas competências fiscalizatórias de acompanhamento da arrecadação, o TCU, em nova auditoria realizada em 2015, requereu novamente o acesso às informações do Siscomex.[20] No entanto, buscando uma solução que relativizasse a controvérsia entre o direito fundamental ao sigilo fiscal dos contribuintes e o interesse público de controle dos atos da Administração Pública, previu a possibilidade de anonimização ou mascaramento dos dados relativos à identificação dos contribuintes, vindo ao encontro da solução adotada no direito europeu já descrita neste trabalho.

No entanto, a RFB mais uma vez deixou de atender à requisição, invocando o sigilo fiscal das informações, visto que os dados revelariam situação econômica dos operadores no comércio exterior, pois continham informações sobre negociações efetuadas, preços praticados pelos agentes e por terceiros envolvidos. Assim, a RFB afirmou que eventual divulgação desses dados ao TCU seria uma afronta ao art. 198 do Código Tributário Nacional.[21]

---

[20] Nessa nova auditoria (processo administrativo TC 005.619/2015-7), buscou-se um maior conhecimento do Siscomex por meio de avaliação dos seus controles internos e a análise da consistência, confiabilidade e integridade dos seus dados. O acesso às informações do sistema possibilitariam a verificação de eventual materialização de riscos relacionados à consistência e legalidade das operações registradas no Siscomex, abrangendo questões como: conformidade legal dos filtros aplicados pelo sistema para emitir anuência automática a pedidos de importação; expedição ou baixa de atos concessórios de *drawback* em desconformidade com a legislação pertinente; observância do limite de utilização autorizado no ato concessório de *drawback*; integridade da parametrização dos canais de conferência aduaneira; efetivação de registro de exportação sem anuência de todos os órgãos competentes, entre outros aspectos relevantes relacionados a uma melhor avaliação do sistema.

[21] Ressalta-se que o não atendimento à diligência do TCU acabou por prejudicar os objetivos da fiscalização, conforme dispõe a equipe técnica do TCU no Relatório do Acórdão 785/2016-TCU-Plenário, que julgou inicialmente o processo TC 005.619/2015-7: "147. Acerca dos procedimentos propostos na fase de planejamento deste trabalho a serem aplicados nos sistemas Siscomex Importação e Seleção Parametrizada, importa dizer que eles foram prejudicados diante da recusa da SRFB em disponibilizar as bases de dados solicitadas sob a alegação de infringir o sigilo fiscal estatuído no art. 198 do Código Tributário Nacional (Lei 5.172/1996). A recusa, além de prejudicar a execução dos procedimentos relacionados a estes dois sistemas, trouxe prejuízos ao cruzamento de dados que se pretendia executar entre as bases de importações realizadas sob o regime de drawback fornecidas pelo MDIC e a base de

Diante dessa nova negativa no fornecimento dos dados, a equipe de auditoria do TCU ofereceu novamente representação por sonegação de informações (processo administrativo TC 017.090/2015-6). Após a análise da devida defesa apresentada pela RFB, o TCU considerou indevida a negativa de fornecimento dos dados. Em resumo, as razões apresentadas pelo TCU foram as seguintes:

> a) o objetivo não é o de auditar a situação econômica de qualquer contribuinte, mas a própria Receita, seus sistemas informatizados, seus procedimentos e seus gestores;
> b) não se pode admitir que a Receita Federal invoque o sigilo fiscal para tentar excluir os seus próprios atos, procedimentos e gestores da fiscalização pelo TCU;
> c) a situação é diversa da tratada no MS 27.091 (em que o Ministro Gilmar Mendes deferiu pedido de medida liminar para suspender a eficácia do Acórdão 1.835/2007–TCU–Plenário) "porque, conforme mencionado anteriormente, o ofício de requisição da equipe de auditoria do TCU expressamente solicitou à RFB que mascarasse, ou seja, que omitisse qualquer informação que pudesse levar à identificação do importador";
> d) a técnica de mascaramento resguarda a privacidade do contribuinte, não havendo motivos para se falar em sigilo fiscal neste caso. (BRASIL, TCU, 2016b)

Nesse sentido, foi determinada a apresentação das informações pela RFB no prazo de 15 dias, conforme constante no Acórdão n. 1958/2015-TCU-Plenário. Contra essa decisão, a RFB interpôs recurso alegando que a anonimização dos dados não é um meio eficaz de preservação do sigilo, pois existe a possibilidade do emprego de técnicas de reidentificação, o que tornaria possível a violação do sigilo fiscal.

O TCU negou provimento a esse recurso, conforme o Acórdão n. 1391/2016-TCU-Plenário, mantendo a determinação de apresentação das informações pelo órgão fiscal. Os argumentos da Egrégia Corte de Contas para essa decisão foram basicamente os seguintes:

1) Mesmo considerando o sigilo fiscal um direito fundamental, não existem direitos absolutos, sendo que esse princípio deve ser devidamente

dados de importações da SRFB, entre outros procedimentos pertinentes à auditoria." (BRASIL, TCU, 2016a)

relativizado quando contraposto ao interesse público da devida fiscalização das atividades de arrecadação pelos órgãos de controle;

2) Diante da omissão legislativa do nosso país em resolver essa controvérsia, a técnica de anonimização ou mascaramento dos dados, já adotada no direito europeu, é uma solução capaz de harmonizar esse conflito;

3) Ainda que seja possível a técnica de reidentificação, considera-se que a técnica de anonimização oferece proteção razoável diante do tempo e esforço demasiados para fazer a reidentificação dos dados considerando o estágio tecnológico atual.

Entende-se correta a decisão do TCU nesse caso analisado, pois, diante da controvérsia existente entre o sigilo fiscal e a necessidade de acesso à informação para um adequado controle da Administração Pública, conforme já explanado neste trabalho, a técnica de anonimização dos dados, já devidamente regulada no direito europeu, é uma boa solução para ser adotada no direito brasileiro. Ressalta-se mais uma vez que a analogia também é considerada como uma das fontes de direito no Brasil, podendo ser utilizada no caso de ausência de normas que regulem adequadamente a questão.

No entanto, o TCU foi ainda mais além. Com vistas à verificar à razoabilidade do mascaramento dos dados, utilizou o postulado da proporcionalidade para verificar se essa solução era adequada para a devida harmonização dos preceitos constitucionais envolvidos, como será visto a seguir.

5. A ADEQUAÇÃO DA ANONIMIZAÇÃO DE DADOS PELO TESTE DA PROPORCIONALIDADE

Quando algum órgão estatal atua no exercício de suas competências – no caso o TCU no exercício de sua competência constitucional de realizar o controle externo da Administração Pública, corre o risco de atuar de maneira desproporcional, afetando outros direitos fundamentais, como, no caso em análise, o direito ao sigilo fiscal dos contribuintes. Uma das técnicas utilizadas para saber se a atuação extrapolou os limites razoáveis é a utilização do

princípio da proporcionalidade como parâmetro de avaliação, desenvolvido pelo doutrinador alemão Robert Alexy.

De acordo com esse autor (2011, p. 111), a própria natureza principiológica dos direitos fundamentais implica a máxima da proporcionalidade como forma de sopesamento em caso de colisão com princípios antagônicos. Isso porque, segundo ele, “princípios são mandamentos de otimização em face das possibilidades jurídicas e fáticas”. Para a otimização dos interesses em conflito, portanto, o teste de proporcionalidade é solução bastante adequada.

Outro autor que defende o princípio da proporcionalidade como fundamento no momento da hierarquização de princípios fundamentais em conflito é Juarez Freitas. No entanto, ressalta a necessidade de que os princípios jurídicos, quando tiverem que preponderar um sobre o outro, devem salvaguard o íntimo dos valores em colisão. (FREITAS, 2010, p. 198-199)

De acordo com Sarlet, a doutrina e a jurisprudência nacionais vêm aceitando como critério de controle da legitimidade constitucional de medidas restritivas, no âmbito da proteção dos direitos fundamentais, a aplicação desse princípio, que se desdobra em três subcritérios: adequação ou conformidade, necessidade ou exigibilidade e proporcionalidade em sentido estrito. Segundo esse doutrinador, a adequação seria o controle de “idoneidade técnica”, ou seja, se avalia se aquele meio utilizado é adequado para se almejar o fim buscado. Já a necessidade seria a avaliação se aquele meio utilizado é o “menos gravoso para o direito objeto de restrição”. Por fim, na proporcionalidade em sentido estrito, se busca responder se “as vantagens causadas pela promoção de determinado fim (ou fins) são proporcionais às desvantagens causados pela adoção do meio, ou seja, as restrições impostas aos direitos fundamentais”. (SARLET; MARINONI; MITIDIERO, 2016, p. 390-392)

Com vistas a aplicar o postulado da proporcionalidade no caso concreto, o TCU sujeitou à questão aos três subcritérios mencionados. Quanto à adequação, a Corte Federal de Contas expôs que o acesso aos dados, mesmo mascarados, possibilita o fim de avaliar a conduta administrativa da RFB,

dando eficácia ao preceito constitucional previsto no art. 70, parágrafo único, que submete a atividade arrecadatória dos órgãos fiscais ao controle externo. Em relação à necessidade, concluiu-se que o acesso aos dados identificáveis contendo informações sensíveis dos titulares dos dados, como CPF e CNPJ, seria medida bem mais gravosa que a alternativa de fornecimento dos dados anonimizados, que é uma solução que não traz prejuízos insuperáveis nem à fiscalização realizada pelo TCU tampouco à privacidade do contribuinte, não se vislumbrando alternativa menos gravosa para o exercício da atribuição fiscalizatória. Por fim, em análise à proporcionalidade em sentido estrito, constatou-se que os benefícios da medida superam seus inconvenientes, visto que o valor fundamental de controle da atividade administrativa da arrecadação e a menor restrição ao direito à privacidade pela anonimização restam atendidos. (BRASIL, TCU, 2016b)

Como bem explanado pela equipe técnica do TCU, a anonimização dos dados se adéqua aos três subcritérios da proporcionalidade. Ainda, conclui-se que o mascaramento das informações permite preservar o núcleo essencial do direito ao sigilo fiscal, uma vez que torna bastante improvável a identificação dos dados pessoais relativos aos contribuintes. Assim, a intimidade dos princípios em colisão é protegida.

Ademais, considera-se o TCU um órgão capaz de manusear as informações com a devida segurança, possuindo os devidos mecanismos para coibir eventuais tentativas de reidentificação ou acessos não autorizados. Ressalta-se que, já há alguns anos, o TCU vem adotando técnicas avançadas de análise e tratamento de dados da Administração Pública, já possuindo diversos trabalhos relevantes.[22] Com vistas a assegurar o adequado tratamento e a segurança das informações, a Corte Federal de Contas inclusive

[22]Dentre os trabalhos relevantes de análise de dados feitos pelo TCU nos últimos anos, destacam-se três fiscalizações que resultaram na verificação de irregularidades bastante relevantes na concessão de benefícios no âmbito do Programa Bolsa Família, na concessão de benefícios previdenciários no âmbito do Regime Geral de Previdência Social e na seleção de beneficiários no Programa Nacional de Reforma Agrária (Acórdãos 1009/2016-TCU-Plenário, 718/2016-TCU-Plenário e 775/2016-TCU- Plenário). Além disso, destaca-se a elaboração de um modelo preditivo de análise de riscos acerca das transferências voluntárias a partir da extração de dados do Sistema de Gestão de Convênios e Contratos de Repasse. Mais considerações a respeito, *vide*: REIS, Fernando Simões dos. O modelo preditivo de análise de riscos e a fiscalização das transferências voluntárias pelo TCU. Interesse Público – IP, Belo Horizonte, ano 18, n. 98, p. 193-209, jul./ago. 2016.

estabeleceu práticas internas consolidadas na Política Corporativa de Segurança da Informação do Tribunal de Contas da União (PCSI/TCU).[23]

Por último, salienta-se que, apesar do STF não ter analisado a nova determinação do TCU à RFB de apresentação das informações, podendo a apresentação dos dados se dar de forma anonimizada, o caso foi alvo de consideração no julgamento do Mandado de Segurança n. 27.091 pelo STF. No voto do Ministro Relator Luís Roberto Barroso, foi ressaltada a adequação da nova forma de compartilhamento de dados proposta pelo TCU, distinguindo a situação analisada no Acórdão 1.391/2016-TCU-Plenário da situação analisada no *writ*, que abrangia apenas a decisão do TCU prolatada no Acórdão n. 1.835/2007-TCU-Plenário, quando a Corte Federal de Contas determinou a apresentação dos dados de forma irrestrita. A respeito disso, assim se pronunciou o Ministro Relator:

> 17. Por fim, ressalto que, em julgado recente (Acórdão nº 1.391/2016), o TCU alterou sua perspectiva a respeito do tema, requisitando da Secretaria da Receita Federal do Brasil o compartilhamento de dados "anonimizados", isto é, com ocultação da identidade dos sujeitos passivos. Essa técnica, numa primeira análise, parece viabilizar a concordância prática entre a garantia de sigilo fiscal e a necessidade de controle da administração tributária.
> 18. Entretanto, como já exposto, no presente mandado de segurança o ato coator consiste em requisição ampla e irrestrita de informações da Receita Federal do Brasil que incluem dados ínsitos à privacidade dos contribuintes. Nesse formato, a requisição é inconstitucional. (BRASIL, STF, 2017)

Portanto, o próprio STF, mesmo que em análise não aprofundada, parece concordar com a providência do TCU para uma adequada solução para a colisão entre o direito fundamental ao sigilo fiscal e a necessidade de controle externo da RFB em sua função precípua de arrecadar tributos.

CONCLUSÃO

Pelo exposto, ainda que o direito fundamental à proteção dos dados seja um direito fundamental, que tem um âmbito de proteção maior em relação

[23]A respeito da Política Corporativa de Segurança da Informação do TCU, acessar o link: <http://portal.tcu.gov.br/biblioteca-digital/pcsi-politica-corporativa-de-seguranca-da-informacao.htm>. Acesso em 4 de junho de 2017.

a outros direitos, essa proteção não pode ser considerada absoluta, principalmente quando colidente com o interesse público de manipulação das informações com vistas ao aumento da eficiência da máquina estatal. Quando houver essa colisão de princípios constitucionais, deve ser adotada uma solução que permita uma relativização dos interesses em jogo, sem que se fira o núcleo fundamental desses direitos.

No caso do conflito entre o direito ao sigilo fiscal e o interesse público de fiscalização da atividade arrecadatória, diante da inexistência de norma infraconstitucional que regule o compartilhamento das informações, buscou-se no direito europeu, por analogia, a solução da controvérsia, pois reconhecidamente a Europa já avançou bastante na matéria de proteção de dados pessoais. A partir desse estudo, vislumbrou-se que a anonimização dos dados é uma alternativa considerada adequada para conciliar os interesses conflitantes, ou seja, permite o processamento das informações pessoais por um órgão estatal sem comprometer o núcleo essencial do sigilo dos dados coletados.

Ainda, demonstrou-se que a solução da anonimização dos dados é adequada ao direito nacional, inclusive já tendo sido utilizada em caso concreto pelo TCU para acesso a informações de sistema da RFB. Na análise efetuada pela Corte Federal de Contas, inclusive foi demonstrada a pertinência de utilização dessa solução mediante o teste da proporcionalidade.

No entanto, mesmo que a analogia ao direito comparado possa ser utilizada como fonte de direito e que já haja um certo reconhecimento pelo STF dessa solução, entende-se que a regulamentação por lei da matéria é essencial para o reconhecimento da solução da anonimização. Somente dessa forma será dada a devida segurança jurídica tanto aos detentores das informações como aos órgãos públicos para uma adequada manipulação dos dados sem ferir o núcleo da privacidade dos indivíduos, evitando-se, assim, possíveis questionamentos judiciais. .

REFERÊNCIAS

ALEXY, Robert. **Teoria dos Direitos Fundamentais**. Tradução: Virgílio Afonso da Silva. 5 ed. São Paulo: Malheiros, 2011.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro:: Renovar, 2006.

FREITAS, Juarez. **A interpretação sistemática do direito**. 5 ed. São Paulo: Malheiros, 2010.

GAYO, Miguel Recio. ***Protección de datos personales e innovación: ¿(In) compatibles?*** 1 ed., Editorial Reus: Madri, 2016.

MENDES, Laura Schertel. O direito fundamental à proteção de dados pessoais. **Revista de Direito do Consumidor**, vol. 79, jul./set., 2011, p. 45-81.

MIRANDA, Victor. O direito à privacidade na era digital e as tutelas assecuratórias. **Fórum de Direito Civil**, Belo Horizonte, ano 5, n. 12, mai./ago., 2016, pp.97-121.

NAVARRO, Ana Maria e LEONARDOS, Gabriela. **Privacidade Informacional**: origem e fundamentos no Direito Norte-Americano. In: CONPEDI/UFF. (Org.). XXI Congresso Nacional do CONPEDI/UFF. 1ed.: FUNJAB, 2012, p. 305

OTTO Y PARDO, Ignacio de. **La Regulación del ejercício de lós derechos y Libertades.** Madrid:Cuadernos Civitas. 1988. p. 110.

REIS, Fernando Simões dos. O modelo preditivo de análise de riscos e a fiscalização das transferências voluntárias pelo TCU. **Revista Interesse Público – IP**, Belo Horizonte, ano 18, n. 98, p. 193-209, jul./ago. 2016.

RODOTÀ, Stefano. **A vida na sociedade de vigilância**: a privacidade hoje. BODIN DE MORAES, Maria C. (org.). DONEDA, Danilo e DONEDA, Luciana Cabral (trads.). Rio de Janeiro: Renovar, 2008. p. 17

RUARO, Regina Linden, RODRIGUES, Daniel Piñeiro. O direito à proteção de dados pessoais na sociedade de informação. **Revista Direito, Estado e Sociedade**, 36, (jan/jun de 2010). pp. 178-199.

SARLET, Ingo. **A eficácia dos direitos fundamentais**: uma teoria dos direitos fundamentais na perspectiva constitucional. 12 ed. Porto Alegre: Livraria do Advogado, 2015. p. 80

SARLET, Ingo, MARINONI, Luiz Guilherme, MITIDIERO, Daniel. **Curso de direito constitucional**. 5 ed. São Paulo: Saraiva, 2016.

WARREN, Samuel; BRANDEIS, Louis. *The right to privacy*. 4 **Harvard Law Review**, 193, 1890. p. 193-220. Disponível em: <http://www.english.illinois.edu/-people-/faculty/debaron/582/582%20readings/right%20to%20privacy.pdf> Acesso em 3 mai. 2017.

LEGISLAÇÃO E JURISPRUDÊNCIA

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil de 1988**. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm>. Acesso em 25 de maio de 2017.

_____. **Decreto-Lei n. 4.657, de 4 de setembro de 1942**. Planalto. Lei de Introdução às normas do Direito Brasileiro. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/Del4657compilado.htm>. Acesso em 2 de junho de 2017.

_____. **Lei n. 5.172, de 25 de outubro de 1996**. Planalto. Dispõe sobre o Sistema Tributário Nacional e institui normas gerais de direito tributário aplicáveis à União, Estados e Municípios. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/L5172Compilado.htm>. Acesso em 25 de maio de 2017.

_____. **Lei n. 8.443, de 16 de julho de 1992.** Planalto. Dispõe sobre a Lei Orgânica do Tribunal de Contas da União e dá outras providências. Disponível em: <http://www. planalto.gov.br/ccivil_03/Leis/L8443.htm>. Acesso em: 6 de maio de 2017.

_____. Senado Federal. **Projeto de Lei do Senado nº 330/2013 – Emenda nº 31 – CCT/CMA (Substitutivo)**. Estabelece princípios, garantias, direitos e obrigações referentes à proteção, ao tratamento e ao uso de dados pessoais. Disponível em: <https://legis.senado.leg.br/sdleg-getter/documento?dm=5111559&disposition=inline >. Acesso em: 29 de maio de 2017.

_____. Supremo Tribunal Federal. **Mandado de Segurança 27.091 Distrito Federal**. Decisão monocrática do Ministro Luís Roberto Barroso que julgou o Mandado de Segurança 27.091 Distrito Federal. Brasília, 30 mar. 2017. Disponível em: <http://www.stf.jus.br/portal/processo/verProcessoPeca.asp?id=311527228&tipoApp=.pdf >. Acesso em: 29 de maio de 2017.

_____. Tribunal de Contas da União. **Acórdão 1835/2007 – Plenário (TC 025.686/2006-7)**. Relator: Ministro Marcos Vinicios Vilaça. Brasília, em 5/9/2007. Disponível em: <https://contas.tcu.gov.br/pesquisaJurisprudencia/#/detalhamento/11/%252a/NUMACORDAO%253A1835%2520ANOACORDAO%253A2007%2520COLEGIA

DO%253A%2522Plen%25C3%25A1rio%2522/DTRELEVANCIA%2520desc%252C%2520NUMACORDAOINT%2520desc/false/1/false > Acesso em 25 de setembro de 2017.

_____. Tribunal de Contas da União. **Acórdão 1958/2015 – Plenário (TC 017.090/2015-6)**. Relator: Ministro Raimundo Carreiro. Brasília, em 5/9/2007. Disponível em: <https://contas.tcu.gov.br/pesquisaJurisprudencia/#/detalhamento/11/%252a/NUMACORDAO%253A1958%2520ANOACORDAO%253A2015%2520COLEGIADO%253A%2522Plen%25C3%25A1rio%2522/DTRELEVANCIA%2520desc%252C%2520NUMACORDAOINT%2520desc/false/1/false> Acesso em 5 de agosto de 2017.

_____. Tribunal de Contas da União. **Acórdão 785/2016 – Plenário (TC 005.619/2015-7)**. Relator: Ministro Raimundo Carreiro. Brasília, em 6/4/2016. Disponível em: <https://contas.tcu.gov.br/pesquisaJurisprudencia/#/detalhamento/11/%252a/PROC%253A00561920157%2520COLEGIADO%253A%2522Plen%25C3%25A1rio%2522/DTRELEVANCIA%2520desc%252C%2520NUMACORDAOINT%2520desc/false/2> Acesso em 25 de maio de 2017.

_____. Tribunal de Contas da União. **Acórdão 1391/2016 – Plenário (TC 017.090/2015-6)**. Relator: Ministro Walton Alencar Rodrigues. Brasília, em 1/6/2016. Disponível em: <https://contas.tcu.gov.br/pesquisaJurisprudencia/#/detalhamento/11/%252a/NUMACORDAO%253A1391%2520ANOACORDAO%253A2016%2520COLEGIADO%253A%2522Plen%25C3%25A1rio%2522/DTRELEVANCIA%2520desc%252C%2520NUMACORDAOINT%2520desc/false/1>. Acesso em 25 de maio de 2017.

UNIÃO EUROPEIA. **Carta dos Direitos Fundamentais da União Europeia, de 18 de dezembro de 2000**. Disponível em: <http://www.europarl.europa.eu/charter/pdf/text_pt.pdf >. Acesso em 25 de maio de 2017.

_____. **Convenção Europeia dos Direitos do Homem** (Convenção para a Protecção dos Direitos do Homem e das Liberdades Fundamentais, de 4 de abril de 1950). Disponível em: <http://www.echr.coe.int/Documents/Convention_POR.pdf>. Acesso em 30 de maio de 2017.

_____.Convenção 108 para a Proteção das Pessoas relativamente ao Processamento Automático de Dados Pessoais, de 28 de janeiro de 1981. Disponível em: <http://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680078b37>. Acesso em 30 de maio de 2017.

_____.Diretiva 46 do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz

respeito ao tratamento de dados pessoais e à livre circulação desses dados. Disponível em: <http://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:31995L0046&qid=1496439211141&from=EN >. Acesso em 30 de maio de 2017.

_____.**Manual para a legislação europeia de proteção de dados**. Disponível em: <http://fra.europa.eu/sites/default/files/fra-2014-handbook-data-protection-pt.pdf >. Acesso em 30 de maio de 2017.

_____. **Regulamento (EU) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados)**. Disponível em: <http://eur-lex.europa.eu/legal-content/pt/TXT/PDF/?uri=CELEX:32016R0679&from=EN> Acesso em 25 mai. 2017.

UNITED STATES. Supreme Court. **Berger v. New York**, 388 U.S. 41, 1967. Disponível em: <https://supreme.justia.com/cases/federal/us/388/41/case.html >. Acesso em 14 nov. 2017.

_____. Supreme Court. **Katz v. United States**, 389 U.S. 347, 1967. Disponível em: <**https://supreme.justia.com/cases/federal/us/389/347/case.html**>. Acesso em 19 jan. 2018.