



## O direito fundamental à proteção de dados e o poder público: o caso do programa alagoano Nota Fiscal Cidadã

*The fundamental right to data protection and public power: the case of the program for tax-evasion prevention of the state of Alagoas*

Ricardo Schneider Rodrigues <sup>a,\*</sup> 

Larissa Nunes de Melo Azevedo <sup>b</sup> 

Larissa de Oliveira Félix Rodrigues Pereira <sup>c</sup> 

**RESUMO:** A pesquisa se propõe a avaliar se o poder público vem conferindo os cuidados necessários à preservação do Direito Fundamental à Proteção de Dados dos contribuintes alagoanos participantes do Programa Nota Fiscal Cidadã. A partir dos métodos dedutivo e explicativo, através de um perfil qualitativo de revisão bibliográfica, foi examinado o âmbito de proteção do referido direito, especialmente após o advento da Lei Geral de Proteção de Dados. Foi possível constatar que o programa apresenta um déficit quanto à proteção de dados pessoais dos participantes. O fortalecimento da capacidade arrecadatória do Estado não é excludente da necessária proteção dos dados pessoais colhidos junto aos contribuintes. É importante compatibilizar a atividade estatal com o respeito a esse direito fundamental.

**Palavras-chave:** Direitos Fundamentais; Proteção de Dados; Poder Público; Nota Fiscal Cidadã.

**ABSTRACT:** The research aims to assess whether the government has been providing the necessary care to preserve the Fundamental Right to Data Protection of State of Alagoas taxpayers participating in the “Nota Fiscal Cidadã” tax-evasion prevention program. From the deductive and explanatory methods, through a qualitative profile of bibliographic review, the scope of protection of that right was examined, especially after the advent of the General Data Protection Law. It was possible to verify that the program has a deficit regarding the protection of the participants' personal data. The strengthening of the State's collection capacity is not exclusive to the necessary protection of personal data collected from taxpayers. It is necessary to make state activity compatible with respect for this fundamental right.

**Keywords:** Fundamental Rights; Data Protection; Public Power; Program for Tax-evasion Prevention.

---


<sup>a</sup> Programa de Pós-Graduação em Direito, Centro Universitário Cesmac, Maceió, AL, Brasil.

<sup>b</sup> Escritório Martorelli Advogados, Maceió, AL, Brasil.

<sup>c</sup> Prefeitura de Piranhas, Piranhas, AL, Brasil.

\* Correspondência para/Correspondence to: Ricardo Schneider Rodrigues. E-mail: prof.ricardo.schneider@gmail.com.

Recebido em/Received: 30/03/2021; Aprovado em/Approved: 15/06/2021.

Artigo publicado em acesso aberto sob licença [CC BY 4.0 Internacional](https://creativecommons.org/licenses/by/4.0/) 

## INTRODUÇÃO

A intensa desconstrução de barreiras geográficas a partir do frenético processo de diálogo e trocas entre pessoas em um mundo globalizado modificou de forma significativa as relações sociais. Para Castells (2011), as novas tecnologias de comunicação e informação impulsionam a difusão de inovações na estrutura social, o que facilita a comunicabilidade dos mais variados assuntos pelas vias virtuais.

Tal fenômeno, contudo, colaborou para a difusão facilitada de dados sensíveis nas mais diversas redes. Atualmente, desde os serviços mais simples prestados por aplicativos *on-line* até as ferramentas virtuais que se tornaram indispensáveis no trabalho cotidiano, todos exigem a disponibilização de informações do interessado como condição de acesso às respectivas plataformas.

Nesse contexto, não apenas a vida em seu aspecto particular está submetida a essa situação de potencial risco à intimidade e privacidade do consumidor. As relações em face do poder público também estão inseridas nessa problemática conjuntura em que muitas informações são cedidas pelos cidadãos sem, contudo, conhecerem as cautelas devidas em relação ao armazenamento e uso desses dados.

Exemplo disso ocorreu no Tribunal Superior Eleitoral. Em 2013 a Corte chegou a firmar um acordo de cooperação técnica com a empresa Serasa – que analisa risco de crédito – para repassar as informações cadastrais de 141 milhões de eleitores em troca da certificação digital dos servidores do tribunal (Bramatti 2013). Caso fosse concretizada a referida transação, ocorreria uma violação do princípio da finalidade – incorporado por diversos autores ao conteúdo do direito fundamental à proteção de dados e, inclusive, expressamente consagrada na posterior Lei 13.709/2.018 (Brasil 2018) –, segundo o qual “qualquer utilização dos dados pessoais deve obedecer à finalidade comunicada ao interessado antes da coleta de seus dados” (Doneda 2011, p. 100).

Em outro caso, uma pesquisa analisou diversos programas fiscais voltados ao aumento da arrecadação tributária nos Estados, os quais armazenam dados detalhados de consumo de seus contribuintes, tendo sido constatada a ausência de transparência sobre a proteção das informações e de segurança do próprio sistema, em relação ao seu uso, a uma eventual transmissão para terceiros e ao descarte dos dados (Machado, Bioni 2016).

Neste contexto, afigura-se relevante avaliar como o poder público vem lidando com a temática da proteção de dados pessoais fornecidos pelos cidadãos para as mais diversas finalidades e, em muitos casos, sem as cautelas que a natureza dessas informações impõe. Tal preocupação se tornou ainda maior diante do longo silêncio legislativo ante a matéria que ora se discute, porquanto até agosto de 2018 não havia no Brasil um posicionamento legal padronizado e uniformizado que versasse exclusivamente sobre os pontos relevantes ao deslinde da controversa disponibilização de dados pessoais a, principalmente, pessoas jurídicas de direito público – as quais estão estritamente vinculadas às inflexíveis disposições normativas, segundo o princípio da legalidade.

Como forma de compreender melhor essa realidade, a presente investigação recaiu sobre o Programa Nota Fiscal Cidadã, promovido pelo Estado de Alagoas, por intermédio da respectiva Secretaria da Fazenda (Sefaz/AL). A pesquisa se propõe a avaliar se o poder público estadual vem conferindo ao referido programa os cuidados necessários a uma proteção mínima desse direito fundamental dos contribuintes alagoanos. Parte-se da hipótese de que não há um tratamento adequado para resguardar os dados fornecidos pelos contribuintes/consumidores, conforme consta na mencionada pesquisa realizada por Machado e Bioni (2016).

Valendo-se dos métodos dedutivo e explicativo, através de um perfil qualitativo de revisão bibliográfica, delimitou-se a análise sob três perspectivas no que se refere ao caráter constitucional e fundamental do direito à proteção de dados: a primeira, oriunda do direito americano, em que a proteção de dados se extrai do Direito à Privacidade; depois, com base no Direito Alemão, o direito a dados assegurados se origina do livre desenvolvimento da personalidade; e, por último, a viabilidade de se entender a garantia ora discutida enquanto um direito fundamental autônomo, ante a permissiva postura adotada pela Constituição Federal de 1988 (Brasil 1988) por meio da cláusula de abertura material. Assim, o método comparativo foi utilizado de forma auxiliar para uma melhor compreensão do direito fundamental à proteção de dados a partir da perspectiva de outros países, em especial dos Estados Unidos e da Alemanha.

Passo seguinte correspondeu ao exame das disposições da Lei nº 13.709/2018 (Brasil 2018) – Lei Geral de Proteção de Dados – LGPD – no que se refere ao uso de dados pessoais pelo poder público. Dessa forma, buscou-se analisar como o ordenamento jurídico brasileiro salvaguarda o direito à proteção de dados como direito fundamental para definir o seu âmbito de proteção, bem como investigar o conteúdo do Programa Nota Fiscal Cidadã, com o fim de analisar se é conferida uma proteção mínima satisfatória dos dados colhidos e, em caso de proteção deficiente, sugerir medidas de adequação em busca de uma maior concretização do direito fundamental à proteção de dados.

Para a avaliação desse programa, houve uma primeira análise a partir das informações existentes no portal na internet da Sefaz/AL. Em seguida, por meio de um questionário estruturado, enviado à Sefaz via Sistema de Informação ao Cidadão (SIC), buscou-se obter outras informações imprescindíveis para a compreensão acerca de como ocorre o tratamento dos dados coletados, desde quando são recolhidos, passando pelo seu armazenamento e, ao fim, o descarte.

## **A PROTEÇÃO DE DADOS PESSOAIS COMO DIREITO FUNDAMENTAL**

Definir a proteção de dados enquanto um direito autônomo, fundamental e conferir-lhe, portanto, caráter constitucional intangível mostra-se etapa de real importância, não apenas do ponto de vista teórico, mas, principalmente, em virtude das consequências práticas que decorrem de tal classificação. Dessa forma, com base nas disposições axiológicas e até mesmo normativas da Constituição Federal (Brasil 1988),

não há como conferir distinto caráter ao direito à proteção de dados como efetivamente um direito constitucional fundamental, vez que está em salvaguarda de bens expressamente tutelados pelo regime dos direitos humanos acolhidos pela Lei Maior.

Para que se entenda o regime adotado quando da proteção aos dados pessoais, contudo, é preciso que se façam algumas considerações acerca das características e abordagens auferidas, legal e doutrinariamente, ao Direito Constitucional. Ao estabelecer implícita hierarquia entre os produtos do processo legislativo e, dessa maneira, situar as emendas constitucionais como as normas mais relevantes do ordenamento jurídico, a Carta Magna destacou a preferência das normas constitucionais quanto à elaboração das demais normas.

Isso porque, de uma maneira geral, não se pode entender como válida e eficaz a ordem legal que vá de encontro ao que estiver predisposto no âmbito da Constituição da República (Brasil 1988), de onde se extrai a supremacia hierárquica do referido diploma, de modo que

tal característica corresponde ao postulado da supremacia da constituição e de que esta é a expressão da vontade de um poder constituinte, já que as normas constitucionais encontram seu fundamento de validade na própria constituição (Sarlet, Marinoni, Mitidiero 2017, p. 97).

Outra característica relevante é o caráter garantista que deve ser-lhe atribuído, de maneira que a efetividade das normas constitucionais não depende de ratificação externa ou superior, sendo autossuficiente sua organização (Sarlet, Marinoni, Mitidiero 2017).

Assim, para consumir as duas principais características acima mencionadas, foram eleitos princípios gerais que guiam a aplicação da norma constitucional, bem como norteiam o processo legislativo a fim de atender aos propósitos do constituinte. É claro que, tendo em vista o direcionamento que se pretende dar ao presente estudo, não se mostra imprescindível o aprofundamento e o esgotamento do tema, de modo que será abordado apenas aquele que possui estreita relação com o ora discutido, qual seja, o princípio da Dignidade da Pessoa Humana.

De referido princípio, por sua vez, é possível extrair proteções específicas que expressam a preocupação com a vida individual e coletiva dos cidadãos, como, por exemplo, o respeito à intimidade, privacidade, à honra e à imagem, basilares dos direitos da personalidade, também previstos no bojo do Pacto de San José da Costa Rica. Dispõe Marmelstein (2011, p. 139) que:

A ideia básica que orienta a positivação desses valores é a de que nem o Estado nem a sociedade de modo geral devem se intrometer, indevidamente, na vida pessoal dos indivíduos. Inserem-se, nesse contexto, inúmeras prerrogativas de caráter individual-subjetivo, como o direito de buscar a paz de espírito e a tranquilidade, o

direito de ser deixado só (direito ao isolamento), o direito de não ser bisbilhotado, de não ter a vida íntima e familiar devassada, de não ter detalhes pessoais divulgados, nem de ter a imagem e o nome expostos contra a vontade da pessoa.

O direito a dados pessoais protegidos está intimamente relacionado aos direitos da personalidade, muito mais no que diz respeito à privacidade dos indivíduos. Isso porque, dentre as inúmeras possibilidades de visualizá-lo, está o “*the right to be alone*”, o que, em outras palavras, diz respeito ao direito do cidadão em não ser lesado em sua vida íntima por outrem, inclusive pelo Estado, sendo relacionado, até, a um direito ao anonimato – dentro das limitações previstas no entendimento contemporâneo (Sarlet, Marinoni, Mitidiero 2017).

Ainda no que diz respeito a essa relação, fica ainda mais evidente quando analisado o posicionamento de J.J Canotilho e Vital Moreira (*apud* Sarlet, Marinoni, Mitidiero 2017, p. 448) acerca do que se entende constituir o direito à privacidade, de modo que dispõem que:

o direito à reserva da intimidade da vida privada e familiar analisa-se principalmente em dois direitos menores: (a) o direito a impedir o acesso de estranhos a informações sobre a vida privada e familiar e (b) o direito a que ninguém divulgue as informações que tenha sobre a vida privada e familiar de outrem.

Assim, quando se fala em proteção a dados pessoais, é possível visualizar exatamente as duas situações, isto é, primeiro obstar que terceiros tenham acesso além daquilo que o indivíduo não permita que ele tenha; e, segundo: que, de posse de dados permitidos, não sejam divulgados ou utilizados de maneiras distintas da anteriormente acordada. O direito à privacidade e, por ilação lógica, o direito à proteção de dados diz respeito à escolha de cada ser quanto ao que compartilhar e ao que deve permanecer pessoalmente resguardado (Vitale 2014).

A privacidade, portanto, originariamente, esteve a todo tempo ligada à ideia de liberdade, de modo que macular tal direito influencia diretamente nos direitos da personalidade dos cidadãos e, mais a fundo, na dignidade humana do indivíduo violado.

Assim, não há como negar que, inevitavelmente, o direito a dados pessoais resguardados é indissociável do direito à privacidade, o qual está expressamente previsto na Constituição Federal (Brasil 1988). O direito americano, inclusive, consagra a proteção de dados pessoais enquanto uma vertente da privacidade, o mencionado *the right to be alone* também o subsidia, de modo que só se sabe daqueles dados que não afrontam ou maculam os limites individuais de privacidade.

O fato é que, mesmo abarcado pelos amplos conceitos de direito à privacidade – e, ainda, segundo o John L. Mills (*apud* Ruaro, Molinaro 2017), de acordo com o direito americano, exista a esfera chamada de *the personal-information sphere: protecting personal data* incorporada ao que se compreende por privacidade –, ainda assim a quebra de fronteiras tecnológicas exige que dados pessoais possuam um sistema de proteção jurídica próprio e diferenciado, capaz de atingir as peculiaridades modernas.

Por ser uma matéria relativamente recente, contudo, existem posições distintas sobre a origem, existência e autonomia de tal direito – não que a proteção de dados pessoais tenha se tornado uma preocupação além do mundo fático apenas em razão dos

avanços tecnológicos, mas, certamente, seus reflexos ficaram mais evidentes no plano jurídico com a dinamização global e os interruptíveis desenvolvimentos técnico-científicos.

Nesse sentido, o Tribunal Constitucional Federal Alemão, ao julgar as diversas reclamações constitucionais propostas em face da *Volkszählungsgesetz* (Lei do Censo), na década de 80, conferiu eficiente interpretação ao direito discutido. Com a legalização da pesquisa sobre inúmeras informações dos cidadãos, levou-se ao judiciário a inconstitucionalidade da referida lei sob o principal fundamento de que seria uma ofensa ao livre desenvolvimento da personalidade. Apesar de ratificada a constitucionalidade, declarou-se “nulos principalmente os dispositivos sobre a comparação e trocas de dados e sobre a competência de transmissão de dados para fins de execução administrativa.” (Schwabe 2005, p. 234). Restou consignado, em suma que,

A autodeterminação individual pressupõe, porém – mesmo sob as condições da moderna tecnologia de processamento de informação –, que ao indivíduo está garantida a liberdade de decisão sobre ações a serem procedidas ou omitidas e, inclusive, a possibilidade de se comportar realmente conforme tal decisão. (...) Daí resulta: o livre desenvolvimento da personalidade pressupõe, sob as modernas condições do processamento de dados, a proteção do indivíduo contra levantamento, armazenagem, uso e transmissão irrestritos de seus dados pessoais. Esta proteção, portanto, é abrangida pelo direito fundamental do Art. 2 I c. c. Art. 1 I GG. O direito fundamental garante o poder do cidadão de determinar em princípio ele mesmo sobre a exibição e o uso de seus dados pessoais.

Em outras palavras, o indivíduo escolhe quais informações lhe convêm serem públicas ou privadas e, a partir daí, molda sua personalidade para lidar com as situações as quais vivencia, ou seja, irá tornar público o que lhe for conveniente.

Ocorre que, nada obstante a íntima relação que a proteção de dados guarda com o direito à privacidade, na perspectiva do direito americano e, ainda, com o direito ao livre desenvolvimento da personalidade, segundo a ordem jurídica alemã, é possível que também seja visualizada enquanto um direito autônomo, diante da expansão tecnológica na vida humana.

Foi justamente nesse sentido que a Carta dos Direitos Fundamentais da União Europeia consagrou, categoricamente, a constituição de um direito individual fundamental à proteção de dados. No Brasil, contudo, a ideia não passa de uma construção doutrinária, vez que o assunto não é, ainda, de pronto, visível no texto constitucional, bem como a legislação acerca da matéria ainda é recente – timidamente a Carta Magna trouxe, em seu artigo 5º, XII (Brasil 1988), o direito ao sigilo das comunicações de dados.

Frise-se que há um elemento que separa o direito à privacidade do direito à proteção de dados e que, por si só, mostra a necessidade de sistemas autônomos e distintos. Segundo Sarlet, Marinoni e Mitidiero (2017), e é este o posicionamento pacífico no ordenamento jurídico pátrio, a violação ao direito à privacidade não é visualizada de plano, isto é, só será revelada a mácula a tal direito se, analisado o caso concreto, perceber a real ofensa ao bem da vida em discussão.

O direito à proteção de dados difere de tal disposição. Isso porque o sistema jurídico que busca garantir essa proteção é sustentado em princípios que guiam a coleta, o armazenamento e o descarte dos dados obtidos. Assim, a ofensa ao que assenta tais princípios, por si só, já gera a presunção de mácula a um direito do cidadão – o de ter seus dados pessoais protegidos e, subsidiariamente, seu direito à privacidade.

Em correto posicionamento, Ruaro e Molinaro (2017, p. 26) acreditam que a ausência de tratamento expresso constitucional no Brasil não retira o caráter de direito fundamental à proteção de dados e “o simples fato de inexistência de legislação específica que trate do direito à proteção de dados pessoais não pode constituir óbice para que se perfectibilize a sua defesa”.

Rapidamente, inclusive, frisa-se o posicionamento de Sarlet, Marinoni e Mitidiero (2017) no que se refere ao âmbito de proteção do mencionado direito, que estaria configurado em cinco distintas situações: o conhecimento e a possibilidade de acessar os dados já registrados; o sigilo de determinados dados – os quais não devem, sequer, ser conhecidos; conhecimento daqueles que serão responsáveis pela coleta, armazenamento, tratamento e utilização dos dados; a informação quanto ao fim da coleta; e, ainda, a garantia à correção e exclusão de determinados dados.

Ainda nesse sentido, assenta que, indiretamente, a Constituição da República (Brasil 1988) se preocupou em defender o direito em tela quando possibilitou como garantia o *habeas data*, o qual assegura o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público e, ainda, para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo.

São visíveis as aproximações constitucionais com a proteção de dados e, ainda que não haja expressa previsão, não é razoável negar a autonomia de tal direito. Conforme o exposto, ao tempo em que entrava em vigor a atual Constituição Federal (Brasil 1988) é que se discutia no mundo sobre a existência de tal direito, mesmo que congênere a algo que já se encontrava no ordenamento jurídico. Dessa forma, se nem a subsistência da proteção de dados era um entendimento sólido, sequer se poderia falar em sua autonomia enquanto um direito constitucional.

Na presente conjuntura, contudo, as discussões são pacíficas quanto à vigência de um direito à proteção de dados que, inclusive, deve ser respeitado enquanto direito fundamental. E é exatamente nesse toar que se deve ressaltar o caráter garantista e dirigente da Constituição Federal de 1988 (Brasil 1988), de modo que em seu texto restou evidente a preocupação em resguardar o quanto fosse possível bens relevantes aos cidadãos.

É preciso ter em mente que os direitos fundamentais “se encontram em processo permanente de formação, conforme avança a humanidade nos aspectos sociológico, cultural, tecnológico e de desenvolvimento da ciência” (Ribeiro 2000, p. 101). Assim, a dignidade da pessoa humana, enquanto escopo e guia do desdobramento constitucional, somado à própria natureza evolutiva e de não esgotamento dos direitos fundamentais, é claro, previu e assegurou a cláusula de abertura material, como uma “moldura de um processo de permanente aquisição de novos direitos fundamentais” (Sarlet 2015, p. 83).

Dispõe o parágrafo 2º do artigo 5º da Carta Magna (Brasil 1988) que os direitos e garantias nela expressos não excluem outros decorrentes do regime e dos princípios

adotados, ou dos tratados internacionais em que a República Federativa do Brasil seja parte.

Se a proteção de dados pode ser entendida como ramificação do livre desenvolvimento da personalidade ou mesmo da privacidade, direitos que possuem indiscutível teor fundamental ou, ainda, percebendo a preocupação direta da Carta Magna com os bens relacionados ao Direito à Proteção de Dados através de garantias que lhes assegurem a devida proteção, não há como afastar a verdadeira independência do direito à proteção de dados.

Dessa forma, o que se evidencia é a vontade da Constituição Federal (Brasil 1988) em conferir tratamento de resguardo eficaz à coleta e ao tratamento de informações individuais dos cidadãos, razão pela qual outra conclusão não cabe se não pelo entendimento de tal direito como autônomo no ordenamento jurídico pátrio, mesmo porque o próprio constituinte derivado pretende encerrar tais controvérsias e conferir a alegada independência constitucional por meio da Proposta de Emenda à Constituição nº 17 (Brasil 2019).

## **ÂMBITO DE PROTEÇÃO E OS DEVERES ESTATAIS DECORRENTES DO DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS PESSOAIS**

A intensificação na análise dos dados pessoais é uma atividade de risco, pois possibilita a exposição e utilização indevida desses dados. É alarmante o modo como o armazenamento, a transmissão, o processamento e o cruzamento dos dados pessoais gera uma corrente de informações sombrias ao seu titular e, apesar de organizações da sociedade civil e organismos estatais buscarem clarear, por meio da criação de normas, esse vácuo regulatório ainda existe.

Em decorrência desse processo tecnológico, houve um aumento no poder informacional do Estado, uma vez que as políticas públicas e dos programas sociais atingiram uma grande dependência dos dados pessoais do cidadão. As informações colhidas têm um grande valor, tanto para o setor público quanto para o privado, pois a partir dessas coletas é possível formar perfis de comportamento, consumo e até mesmo de características. Nesse cenário existe a necessidade de criação de mecanismos de proteção que possibilitem à pessoa deter conhecimento e controle sobre seus dados.

A esfera de proteção à privacidade, prevista na Constituição Federal (Brasil 1988), busca proteger o indivíduo de invasões de terceiros no campo pessoal e dos dados pessoais. Contudo, o crescimento tecnológico e o elevado processamento de informações pessoais alteraram o sentido clássico de violação, acarretando um perfil moderno e um novo significado do que se entende por privacidade (Ruaro, Molinaro 2017).

Nesse patamar, é pertinente buscar a origem do direito à proteção de dados para, a partir da sua evolução, extrair quais dados devem ser tutelados e como essa proteção deve ocorrer. Danilo Doneda (2011) faz alusão à classificação de Viktor Mayer-Sconberger sobre como se deu o progresso das leis de proteção de dados pessoais.



De início, as leis de proteção de dados pretendiam regular centros elaboradores de dados que realizavam a coleta e a gestão de dados pessoais. Essas leis buscavam a autorização para criação desses bancos de dados e o controle posterior pelos órgãos públicos. A in experiência com tal tratamento e o receio devido à falta de habilidade com o uso desenfreado dessa tecnologia fez com que fossem criados princípios de proteção, abstratos e amplos, focados basicamente na atividade de processamento de dados, além da criação de regras concretas e específicas direcionadas aos agentes responsáveis pelo processamento das informações (Doneda 2011).

Entretanto, essa primeira geração de leis logo se tornou ultrapassada, diante do aparecimento de diversos centros de processamento, o que dificultou o acompanhamento rígido e detalhado que esses centros demandavam. Assim, as novas leis de proteção surgiram, dando liberdade para os próprios cidadãos defenderem seus interesses e seus dados.

A grande necessidade do fornecimento dos dados pessoais pelos cidadãos para sua participação ativa na vida social, porém, motivou uma nova mudança de leis, surgindo uma terceira geração, que continuava focada no cidadão, mas “passou a abranger mais do que a liberdade de fornecer ou não os próprios dados pessoais, garantindo também a efetividade dessa liberdade” (Doneda 2011, p. 7).

Diante desse contexto, Sarlet, Marinoni e Mitidiero (2017) citam a já mencionada decisão do Tribunal Constitucional Federal da Alemanha, proferida em 1983, da qual se extrai a incompatibilidade da dignidade da pessoa humana e do direito ao livre desenvolvimento da personalidade com a não proteção do indivíduo contra uma ilimitada coleta; com o armazenamento, o aproveitamento, a transferência e a divulgação dos dados pessoais.

Assim surgiu a autodeterminação informativa, com a intenção de suprir as desvantagens do cenário de proteção individual existente no período, buscando elevar o padrão coletivo de proteção. Doneda (2011, p. 7-8) explica:

O tratamento dos dados pessoais era visto como um processo, que não se encerrava na simples permissão ou não da pessoa à utilização de seus dados pessoais, porém procurava incluí-la em fases sucessivas do processo de tratamento e utilização de sua própria informação por terceiros, além de compreender algumas garantias, como o dever de informação.

Têmis Limberger (2017, p. 147) sustenta que a autodeterminação informativa foi criada com o objetivo de “garantir aos cidadãos direitos de informação, acesso e controle dos dados que lhes concernem. Essa faculdade não é intrassubjetiva, mas sim uma autodeterminação do sujeito no seio de suas relações com os demais cidadãos e o poder público”.

Em virtude do caráter exclusivo da autodeterminação informativa, criou-se a quarta geração de leis de proteção de dados, com o objetivo de preencher as desvantagens do enfoque individual existente até então. Essas leis, existentes até hoje em vários

ordenamentos jurídicos, mostraram-se necessárias para fortalecer a posição da pessoa em relação às entidades que coletam e processam seus dados (Doneda 2011).

Nessa perspectiva, pode-se extrair da autodeterminação informativa um vínculo entre a dignidade da pessoa humana e a privacidade. Partindo do princípio de que a função sociopolítica da privacidade se estrutura como elemento intrínseco da cidadania, deve-se evidenciar a dignidade, de modo que não haja a redução da pessoa a fins mercadológicos, equilibrando com o respeito à igualdade e, em especial, afastando uma possível interferência não desejada pelo indivíduo (Ruaro, Molinaro 2017).

A partir desse novo conceito de proteção de dados iniciou-se uma discussão quanto à natureza da autodeterminação informativa, se seria um novo direito a ser tutelado ou se tratava de um desmembramento do direito à intimidade, que evoluiu para a proteção de dados pessoais de forma autônoma.

Diante do cenário atual, no qual existem sistemas cada vez mais aperfeiçoados para coleta e tratamento de dados, faz-se imprescindível a existência de uma proteção objetiva dos dados pessoais. Assim, introduzir um comando de proteção de dados pessoais tanto para o Estado quanto para os entes privados é indispensável, de modo que sejam respeitados princípios, direitos e deveres dos indivíduos que têm seus dados coletados.

Afigura-se importante delimitar quais dados devem ser tutelados para garantir ao cidadão proteção em face de seu uso inconsequente. Especialmente em relação àqueles que resultem em uma formação de perfis de consumo e transformem o ser humano em um objeto de valor comerciável, ferindo sua liberdade, privacidade e dignidade.

À frente do que Limberger (2017, p. 148) apresenta, pode-se dizer que o direito à proteção de dados pessoais alcança “todos os dados de caráter pessoal que digam respeito ao cidadão”. Significa dizer que esses dados devem ser objeto de um tratamento legal, com finalidade específica e com consentimento da pessoa interessada.

Na busca de uma tutela sem lacunas em todos os aspectos que envolvem a coleta, armazenamento, tratamento, utilização e transmissão de dados pessoais é possível tomar por base do âmbito de proteção do direito à proteção de dados as seguintes concepções jurídicas indicadas por Sarlet, Marinoni e Mitidiero (2017, p. 512):

o direito de acesso e conhecimento dos dados pessoais existentes em registros (bancos de dados) públicos e privados; b) direito ao não conhecimento, tratamento e utilização e difusão de determinados dados pessoais pelo Estado ou por terceiros, aqui incluído um direito de sigilo quanto aos dados pessoais; c) direito ao conhecimento da identidade dos responsáveis pela coleta, armazenamento, tratamento e utilização dos dados; d) o direito ao conhecimento da finalidade da coleta e eventual utilização dos dados; e) direito a retificação e, a depender do caso, de exclusão de dados pessoais armazenados em banco de dados.

Em harmonia com tais concepções, Danilo Doneda (2011) faz alusão aos princípios que devem ser o pilar de toda norma que procure solucionar o problema referente à proteção de dados pessoais, cabendo ao Estado a função de inseri-los em seu ordenamento. São eles: a) princípio da finalidade: vincula os dados aos fins comunicados ao titular antes da coleta; b) princípio da exatidão: os dados armazenados devem ser fiéis à realidade e devem ser atualizados, conforme a necessidade; c) princípio da publicidade: a existência de um banco de dados com dados pessoais deve ser de conhecimento público; d) princípio do livre acesso: o indivíduo deve ter acesso ao banco de dados em que seus dados estão armazenados, tendo a possibilidade de controlá-los; e) princípio da segurança física e lógica: os dados armazenados devem ser protegidos contra os riscos de seu extravio, destruição, modificação, transmissão ou acesso não autorizado.

Na prática, cumpre reconhecer que todo indivíduo tem o direito fundamental de acessar a informação de todo e qualquer banco de dados que armazene e trate seus dados pessoais. Não se vislumbra a possibilidade de ocorrer o armazenamento dessas informações sem o conhecimento e consentimento do titular. Além disso, o indivíduo necessita ter a seu dispor um meio de se informar sobre registros que contenham informações ao seu respeito e como essas informações são utilizadas. Ao tomar conhecimento de uma informação pessoal armazenada, a possibilidade de retificá-la ou excluí-la, se assim desejar, precisa ser respeitada. Ao titular dos dados é indispensável garantir que as informações colhidas serão utilizadas para o fim anunciado, tomadas as devidas precauções para que não sejam disponibilizados para outros fins sem a anuência do seu titular.

Essas hipóteses são meios de garantir ao cidadão uma proteção mais efetiva e rigorosa às suas informações pessoais. Um registro que não seguir este padrão, exceto nos casos permitidos em lei, não deve ser autorizado, devendo ser considerado uma prática desleal.

No que diz respeito aos dados pessoais e os bancos de armazenamentos existentes, não é por acaso que se faz necessária a implementação de modelos jurídicos mais amplos e rigorosos quanto à proteção dos dados pessoais.

Percebe-se que ao ceder informações para um fim específico, esses dados não podem ser utilizados na formação de perfis, retirando o indivíduo da sua condição de sujeito para se tornar um objeto de valor comercial. Cabe ao Estado instituir medidas que protejam o cidadão diante dos interesses econômicos em torno dos bancos de dados criados, sem nenhum critério de proteção, em virtude da ausência de eficácia na regulamentação dos direitos à proteção de dados. Essencial delimitar a utilização sem o conhecimento ou autorização do titular dos dados, para consolidar a proteção da pessoa e dos direitos fundamentais a ela inerentes no que se refere aos seus dados pessoais.

## A LEI GERAL DE PROTEÇÃO DE DADOS BRASILEIRA

O caráter constitucional da matéria e o âmbito de proteção do direito em discussão, não foram as únicas questões delicadas no trato da proteção de dados pessoais no Brasil. Foram enfrentados cenários turbulentos, decorrentes do longo período de inexistência de vertentes, mesmo que ordinárias, que tratassem acerca da matéria. Essa ausência de normas, por muito tempo, não só impossibilitou a busca do cidadão por segurança em seus dados particulares, como também dificultou relações internacionais entre o Brasil e países da União Europeia. Por exemplo, quando instituições internacionais passaram a negar informações privilegiadas enquanto não houvesse um regulamento uniformizado sobre o tema (Pádua 2018).

Diante da evidente marginalização do Brasil em âmbito internacional, foi publicada em agosto de 2018 a Lei Geral de Proteção de Dados Pessoais (Brasil 2018). Esse microsistema visa uniformizar o tratamento material e processual do objeto em discussão e facilita o efetivo resguardo de dados cedidos a Empresas e à Administração Pública e a proteção de seus titulares.

Daí em diante, as legislações estaduais, por conseguinte, deverão se ajustar aos ditames nela previstos, com destaque para o respeito aos princípios que a norteiam, quais sejam: princípios da finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização e prestação de conta.

Além disso, o Direito à Proteção de Dados ganha cada vez mais destaque social e autonomia no ordenamento jurídico brasileiro. A disseminação descontrolada de informações pessoais mostrou ser um mercado multimilionário e, como consequência, atraiu, em uma escala de tempo curta, a preocupação do Poder Legislativo pátrio.

Tal cenário é evidente, nada obstante o silêncio normativo ocorrido até meados de 2018, mesmo por que, em menos de um ano houve expressiva mobilização no que se refere a tais questões – seja com o advento da Lei nº 13.709/2018 (Brasil 2018), seja com a Proposta de Emenda Constitucional nº 17 (Brasil 2019), não há como afastar o caráter constitucional da matéria em debate.

Inclusive, nesse sentido, insta salientar que a referida lei, corretamente, abraçou em seu bojo todos os posicionamentos teóricos no que se refere às questões axiológicas por ela abrangidas (Ruaro, Molinaro 2017), demonstrando ainda mais a observância legal ao que dispunha a doutrina especializada.

Ademais, o tratamento diferenciado conferido aos dados sensíveis mostra-se como uma medida perfeitamente democrática e, acima de tudo, preocupada em vedar uma lucratividade ilícita por parte daqueles que os detêm, vedando o uso de dados com o fim eminentemente econômico sem a regular observância legal.

Do mesmo modo, igual respaldo merece a preocupação legal na proteção ao consentimento daquele que está informando seus dados pessoais. Esse deve ser expresso, inequívoco e, acima de tudo, livre. A exclusão das informações também está inserida no processo de “tratamento”, tendo a mesma relevância que as cautelas tomadas quando das tratativas iniciais – ou seja, em não havendo mais consentimento, o cidadão não pode ser compelido a manter seus dados sob posse de outrem.

Com posicionamentos bastante similares ao Regulamento da União Europeia, o *General Data Protection Regulation* (GDPR), a norma brasileira se preocupou em estabelecer princípios reguladores das relações jurídicas advindas de cessão de informações pessoais. Além disso, estabeleceu os beneficiários das disposições normativas ao ligeiramente indicar como deve ser feito o tratamento dos dados transferidos – ressalte-se que a LGPD coloca expressamente a cargo de lei posterior o factual tratamento.

Nesse sentido, em observância aos termos da LGPD, o princípio da publicidade restou legalmente visualizado através do princípio da transparência. Por meio dessa norma, assegurou-se aos cidadãos informações completas e acessíveis acerca do tratamento conferido aos dados fornecidos, também amparado pelo princípio do livre acesso.

O princípio da exatidão também foi abarcado através da exigência de qualidade dos dados. Tal imperativo ~~que~~ determina, tanto quanto possível, a atualização das informações coletadas e a fidedigna correspondência entre o que foi dito com o que será armazenado, não sendo permitida a manipulação ou alteração da substância.

O princípio da finalidade é um dos principais guias para o correto tratamento e uso de dados adquiridos. Por força dessa norma, não deve ocorrer o desvirtuamento do consentimento conferido pelo titular – se a concordância foi de uso dos dados para um determinado fim, não podem, portanto, ser utilizados para questões alheias sem novo consentimento expresso do cidadão. O referido princípio também foi recepcionado no microssistema nacional e está intimamente relacionado aos princípios da adequação – segundo o qual deve ser compatível o tratamento conferido com as finalidades informadas ao titular – e da necessidade – que limita o tratamento apenas àquilo que for indispensável à realização da finalidade acordada.

Deve ser entendido, também, como um desdobramento da autodeterminação informativa, a qual “resguarda o titular dos dados contra a utilização indevida de suas informações, coibindo discriminações e controles sociais calcados em bancos de dados que não são de seu conhecimento” (Ruaro, Molinaro 2017, p. 32-33).

Por fim, o princípio da segurança também foi legalmente previsto e, inclusive, excessivamente amparado pelas inúmeras disposições que regulamentam as questões atinentes ao tratamento de dados propriamente ditos.

Essas hipóteses são meios de garantir ao cidadão uma proteção mais efetiva e rigorosa às suas informações pessoais. Salvo por autorização legal, não se mostra apropriada a

manutenção de padrões que violem tais disposições normativas, justamente pelo risco que carregam e pelo caráter desleal que possuem.

## **O PROGRAMA NOTA FISCAL CIDADÃ E A PROTEÇÃO DE DADOS**

O Programa Nota Fiscal Cidadã, anteriormente conhecido como Nota Fiscal Alagoana, é um programa de estímulo aos consumidores, criado em 2008, sob a coordenação da Secretária de Estado da Fazenda de Alagoas (Sefaz/AL). Possui a finalidade de incentivar a exigência da nota fiscal nas compras feitas nos diversos estabelecimentos comerciais, a fim de diminuir a sonegação fiscal no Estado.

O programa se dispõe a devolver até 10% (dez por cento) do ICMS recolhido pelo estabelecimento ao consumidor que informar o CPF ou CNPJ no momento da compra, podendo este escolher a forma como o crédito será devolvido e, ainda, concorrer a prêmios. Para seu devido funcionamento, o consumidor deve realizar um cadastro que armazena seus dados. Toda compra realizada por aquele que se identificar será registrada pormenorizadamente no sistema, criando um perfil de consumo para aquele usuário.

Segundo dados cedidos pela própria Sefaz, em 2018 foram mais de 246 mil consumidores cadastrados, de maneira que esse banco de dados do programa gerou a produção de perfis individuais e detalhados do consumo de milhões de pessoas. Esse banco de dados se inicia no próprio estabelecimento que comercializa o bem consumido e, posteriormente, é transmitido para a base de dados do programa Nota Fiscal Cidadã.

Ao examinar o portal na internet do Programa Nota Fiscal Cidadã, em busca de informações claras sobre como os dados do cidadão são protegidos, não foi constatada nenhuma referência à privacidade ou à proteção dos dados pessoais coletados. Não existem informações sobre a administração dos dados no que se refere a sua proteção e utilização.

Da mesma forma, através da análise das legislações que regulamentam o programa, persistiu o vácuo informacional sobre a proteção oferecida aos dados pessoais dos consumidores que aderem ao programa.

Diante da deficiência de informações no portal do programa, foi realizada nova pesquisa, por meio de questionário destinado à Sefaz, pormenorizando o controle dos dados pessoais cedidos ao programa Nota Fiscal Cidadã. Este levantamento foi exercido por meio do SIC (Serviço de Informação ao Cidadão) viabilizado pela Lei de Acesso à Informação – Lei nº 12.527/2011 (Brasil 2011). Assim, foram submetidas 23 perguntas relacionadas à coleta, ao armazenamento e ao tratamento dos dados fornecidos pelos cidadãos participantes do programa no período de 23 de novembro de 2018 a 6 de fevereiro de 2019.

## Da análise do programa a partir de questionário enviado à Sefaz

Inicialmente, destaca-se que as respostas alcançadas por meio do questionário submetido à Sefaz foram pouco esclarecedoras. Tal fato demonstra uma ausência de políticas de proteção dos dados pessoais.

Perguntou-se qual o destino dos dados quando estes não são mais necessários para as finalidades do Programa e se havia algum descarte. Informaram que os dados são mantidos para rastreabilidade, mesmo após a prescrição dos créditos, e que nos casos de notas fiscais eletrônicas esses dados são armazenados por um período de 50 anos.

Indicaram que os dados de interesse do Programa Nota Fiscal Cidadã, ou seja, os que são armazenados, referem-se ao período da compra, valor total da compra e o CPF do consumidor. Além disso que são armazenados em sistemas de banco de dados específicos do programa.

O consentimento do usuário para a coleta de seus dados é ofertado pela simples inclusão do CPF do consumidor no momento da compra, se tiver realizado o cadastro no site do programa. Desta forma os dados coletados servem para identificação dos créditos a que os cidadãos têm direito.

A disposição normativa, contudo, nos termos da Lei nº 13.709/2018 (Brasil 2018), assim como na Regulamentação Europeia, prevê que o titular dos dados prestados deve expressar que está de acordo com o tratamento das informações para a finalidade que foram recolhidas. Ademais, é facultada, a qualquer tempo, a exclusão dos dados fornecidos – uma vez requerida a exclusão, cessa o consentimento, requisito indispensável ao tratamento dos dados.

No que concerne à disponibilidade e ao livre acesso do usuário sobre seus dados, no entanto, a Sefaz informou que esses estão disponíveis ao usuário no site [nfcidada.sefaz.al.gov.br](http://nfcidada.sefaz.al.gov.br), mediante cadastro. Ocorre que, se o cidadão discordar do armazenamento de algum dado, não tem a opção de excluí-lo, constatando-se que o usuário do programa perde o controle daquilo que foi disponibilizado.

Tal questão está diretamente relacionada ao princípio da finalidade, uma vez que a concordância, nos estritos termos legais, é manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para um fim determinado.

Terminada a finalidade de obtenção dos dados ou cessado o consentimento, esses, de acordo com a LGPD, devem ser eliminados e a forma utilizada pelo controlador para atingir tal fim deve ser comunicada, prezando pela transparência entre as partes e a segurança ao titular.

Quando questionado se os consumidores adeptos ao Programa Nota Fiscal Cidadã são informados sobre a finalidade da utilização de seus dados pelo programa, respondeu-se que as informações estão presentes na Lei 6.991/2008 (Estado de Alagoas 2008b),

Lei 7.793/2016 (Estado de Alagoas 2016) e Decreto 4.073/2008 (Estado de Alagoas 2008a); entretanto, ao analisar as referidas legislações, é possível constatar que elas tratam apenas da funcionalidade do Programa, ausentes informações quanto às políticas de privacidade e proteção de dados pessoais dos usuários.

No que se refere ao acesso dos dados pertencentes aos usuários, que são coletados pelo Programa Nota Fiscal Cidadã, relatou-se que são restritos aos funcionários da Sefaz, estando protegidos pelo sigilo fiscal. Assim, no caso de vazamento de dados ou desvio da finalidade, deve-se seguir o disposto no artigo 198 do Código Tributário Nacional (Brasil 1966).

Ocorre que, diante da ausência de políticas que exerçam um controle interno efetivo, não se sabe quem são os servidores que possuem autorização para acessar os dados fornecidos pelos cidadãos. Resta acreditar no bom exercício do poder discricionário por parte dos gestores do programa.

Além de que, em que pese ter sido informado que os dados são de uso exclusivo do programa, não sendo cedidos para terceiros, vale ressaltar que os comerciantes também detêm posse sobre eles através do detalhamento da nota fiscal. Ou seja, não há como garantir que essas informações não são utilizadas para criação de cadastros privados em que é possível analisar o perfil de consumo de cada cidadão, sem mencionar, ainda, a possibilidade de serem cedidas a seguradoras para cadastros de análise de créditos. Em outras palavras, considerando o longo lapso temporal de vácuo legislativo, os estabelecimentos comerciais que detêm acesso aos dados possuíam a liberdade de tratá-los.

Acerca do armazenamento dos dados dos usuários pelos comerciantes, foi informado que os dados constantes na nota fiscal estão também em posse destes, o que não impede que os estabelecimentos comerciais façam uso das informações ou as disponibilizem para terceiros. Somado a isso, considere-se, ainda, a inexistência de normas de proteção ou determinação expressa para que os dados obtidos no âmbito do programa tenham como finalidade exclusiva o combate à sonegação fiscal e o cálculo dos benefícios tributários para os consumidores cadastrados.

Ademais, questionou-se quais as medidas passariam a ser adotadas diante dos recentes ditames previstos na Lei Geral de Proteção de Dados (Brasil 2018) e, surpreendentemente, a resposta obtida foi a de que “como são tratados como dados sujeitos ao sigilo fiscal, os dados já atendem aos requisitos da Lei”.

Nesse diapasão, percebe-se que o Programa Nota Fiscal Cidadã não atende ao que se espera do Estado em relação aos seus deveres decorrentes do direito fundamental à proteção de dados. Há lacunas quanto às exigências necessárias para se conferir um grau aceitável de proteção.

Questões como o consentimento inequívoco quanto ao uso específico dos dados fornecidos passaram a ser mais rigorosas e, da mesma forma, deverá ser possibilitada ao cidadão a exclusão dos dados que entenda necessária. Mesmo porque reitera-se



que, cessado o consentimento, é imperativo legal a exclusão dos dados fornecidos – o que não ocorre na atual sistemática do programa.

Não basta, ainda, que o tratamento das informações preste observância apenas à legislação tributária, haja vista que, nessa extensão, em nada contribui ao manuseio correto e cauteloso dos dados dos cidadãos cadastrados. O sigilo fiscal em nada se relaciona à proteção que deve ser conferida ao armazenamento de quaisquer dados que identifiquem ou qualifiquem o consumidor.

## CONCLUSÕES

O objetivo deste trabalho consistiu em investigar se o Programa Nota Fiscal Cidadã, promovido pelo Estado de Alagoas, resguarda o direito fundamental à proteção de dados pessoais dos contribuintes alagoanos. Partindo da análise do disposto no texto constitucional até o novo cenário legislativo trazido pela Lei Geral de Proteção de Dados (Brasil 2018), em especial para delimitar o âmbito de proteção desse direito fundamental, avaliou-se o Programa Nota Fiscal Cidadã, à luz das informações obtidas junto ao poder público pelo Sistema de Informação ao Cidadão (SIC).

Foi possível constatar que a regulamentação do programa Nota Fiscal Cidadã está diretamente ligada ao combate da sonegação e ao fortalecimento das funções fiscalizadoras do Estado, existindo, todavia, um déficit na proteção de dados pessoais dos cidadãos. Os procedimentos técnicos e operacionais que regem o programa estão limitados a padrões e protocolos voltados às suas próprias finalidades, com pouca preocupação no que se refere à coleta e proteção dos dados pessoais.

Nesse diapasão, com base na crescente expressão normativa no que se refere à tutela da autodeterminação informativa, percebe-se que a Secretária da Fazenda do Estado de Alagoas pouco atende aos requisitos básicos para uma proteção efetiva dos dados pessoais fornecidos pelos cidadãos, ficando ainda mais deficiente no que tange às exigências legais que passaram a ser cobradas com o advento da Lei nº 13.709/2018 (Brasil 2018).

É pertinente sugerir, por tais razões, medidas voltadas ao resguardo da privacidade e proteção aos dados dos usuários, armazenados nos bancos de dados do programa, em conformidade com o disposto na nova Lei Geral de Proteção de Dados (Brasil 2018), a fim de reduzir a possibilidade de danos à esfera pessoal dos cidadãos/contribuintes cadastrados. Uma primeira medida adequada seria a restrição da coleta e do armazenamento apenas aos dados estritamente necessários às finalidades do programa – combate à sonegação e aprimoramento da fiscalização estatal.

Para uma proteção mais efetiva desse direito fundamental, também caberia ao Estado fornecer previamente informações importantes, como a forma como os dados serão armazenados e o destino que será conferido a eles, antes mesmo da efetivação do cadastro. As questões e riscos relacionados ao trânsito de dados pessoais ainda não

lograram alcançar o devido conhecimento pela sociedade, que desconhece as reais consequências e possibilidades associadas ao uso indevido dessas informações. Caberia ao poder público envidar esforços no sentido de disseminar o conhecimento e evitar riscos desnecessários aos envolvidos.

Outro aspecto relevante que deveria ser incorporado ao programa refere-se à possibilidade de retificação ou exclusão dos dados cadastrados. Enquanto tal medida não se concretizar, contudo, deveria haver uma clara advertência de que não é possível corrigir ou apagar as informações armazenadas, como forma de garantir, por enquanto, o consentimento livre e legítimo daqueles que desejaram participar do programa, bem como os riscos que isso implicará.

É possível concluir, do exposto, que embora o programa de combate à sonegação fiscal seja um instrumento importante e voltado à concretização do interesse público de obter a arrecadação tributária necessária à consecução das diversas políticas públicas a cargo do Estado, não deve servir de instrumento para a mitigação do direito fundamental à proteção de dados pessoais. A rigor, conforme demonstrado, o fortalecimento da capacidade arrecadatória do Estado não é excluyente da necessária proteção dos dados pessoais colhidos junto aos contribuintes. É possível – e, agora, necessário – compatibilizar a atividade estatal com o respeito a esse direito fundamental, a partir da adoção de medidas simples, mas de grande importância para a proteção de todos os envolvidos.

## **FINANCIAMENTO**

O presente trabalho foi realizado com apoio do Centro Universitário CESMAC, através do Programa Semente de Iniciação Científica – PSIC.

## **REFERÊNCIAS**

BRAMATTI, Daniel, 2018. Justiça eleitoral repassa dados de 141 milhões de brasileiros para a Serasa. O Estado de S. Paulo, São Paulo. 6 agosto 2013. [Acesso em 29 março 2021]. Disponível em: <http://politica.estadao.com.br/noticias/geral,justica-eleitoral-repassa-dados-de-141-milhoes-de-brasileiros-para-a-serasa,1061255>.

BRASIL. Lei nº 5.172, de 25 de outubro de 1966. Código Tributário Nacional (CTN). Brasília, DF, Presidência da República. [Acesso em 14 de junho de 2021]. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/leis/l5172compilado.htm](http://www.planalto.gov.br/ccivil_03/leis/l5172compilado.htm).

BRASIL. Constituição da República Federativa do Brasil de 1988. Brasília, DF, Presidência da República. [Acesso em 14 de junho de 2021]. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/constituicao/constituicao.htm](http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm).

BRASIL. Lei nº 12.527, de 18 de Novembro de 2011. Lei de Acesso à Informação (LAI). Brasília, DF, Presidência da República. [Acesso em 29 março 2021]. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2011-2014/2011/lei/l12527.htm](http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm).

BRASIL. Lei nº 13.709, de 14 de Agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF, Presidência da República. [Acesso em 29 março 2021]. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/L13709.htm](http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm).

BRASIL. Proposta de Emenda à Constituição nº 17, de 2019. Brasília, DF, Câmara dos Deputados. [Acesso em 14 de junho de 2021]. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2210757>.

CASTELLS, Manuel, 2010. Globalisation, Networking, Urbanisation: Reflections on the Spatial Dynamics of the Information Age. *Urban Studies* [em linha]. 2010. vol. 47, no. 13.

DONEDA, Danilo, 2011. A proteção dos dados pessoais como um direito fundamental. *Espaço Jurídico* [em linha]. 2011. vol. 12, no. 2, p. 91-108.

ESTADO DE ALAGOAS. Decreto nº 4.073, de 13 de Novembro de 2008<sup>a</sup>. Regulamenta a Lei nº 6.991, de 24 de outubro de 2008, que dispõe sobre a criação do programa de estímulo à cidadania fiscal do estado de Alagoas e dá outras providências. [Acesso em 29 março 2021]. Disponível em: [http://www.econeteditora.com.br/icms\\_al/Decretos/2008/decreto\\_4073\\_2008.php](http://www.econeteditora.com.br/icms_al/Decretos/2008/decreto_4073_2008.php).

ESTADO DE ALAGOAS. Lei nº 6.991, de 24 de Outubro de 2008<sup>b</sup>. Dispõe sobre a criação do Programa de Estímulo à Cidadania Fiscal do Estado de Alagoas, e dá outras providências. Maceió, AL, Governador do Estado. [Acesso em 29 março 2021]. Disponível em: <https://www.legisweb.com.br/legislacao/?id=117753>.

ESTADO DE ALAGOAS. Lei nº 7.793, de 22 de Janeiro de 2016. Altera a Lei Estadual nº 6.991, de 24 de outubro de 2008, que dispõe sobre a criação do Programa de Estímulo à Cidadania Fiscal do Estado de Alagoas, e dá outras providências. Maceió, AL, Governador do Estado. [Acesso em: 29 março 2021]. Disponível em: <https://www.legisweb.com.br/legislacao/?id=315685>.

LIMBERGER, Têmis, 2017. Mutações da privacidade e a proteção dos dados pessoais. Em: *Privacidade e Proteção de Dados Pessoais na Sociedade Digital*. Porto Alegre, RS: Editora Fi, 2017, p. 145-168.

MACHADO, Jorge, BIONI, Bruno Ricardo, 2016. A proteção de dados pessoais nos programas de Nota Fiscal: um estudo de caso do “Nota Fiscal paulista”. *Liinc em Revista* [em linha]. 2016. vol. 12, no. 2, p. 350-364. [Acesso em 29 março 2021]. Disponível em: <http://dx.doi.org/10.18617/liinc.v12i2.919>.

MARMELSTEIN, George, 2011. Curso de Direitos Fundamentais. São Paulo, SP: Atlas.

ESTADO DE ALAGOAS, 2021. Nota fiscal cidadã. [Acesso em 29 março 2021]. Disponível em: <http://nfcidada.sefaz.al.gov.br/>.

RIBEIRO, Diógenes V. Hassan, 2000. O Permanente Reconhecimento dos Direitos Fundamentais. *Revista da AJURIS* [em linha]. 2000. vol. 22. [Acesso em 29 março 2021]. Disponível em: <https://bit.ly/3wa8Tve>.

RUARO, Regina Linden, MOLINARO, Carlos Alberto, 2017. Conflito real ou aparente de interesses entre o direito fundamental à proteção de dados pessoais e o livre mercado. Em: *Privacidade e Proteção de Dados Pessoais na Sociedade Digital*. Porto Alegre, RS: Editora Fi, 2017. p. 13-45.

SARLET, Ingo Wolfgang, MARINONI, Luiz Guilherme, MITIDIERO, Daniel, 2017. Curso de Direito Constitucional. São Paulo, SP: Saraiva.

SARLET, Ingo Wolfgang, 2015. Eficácia dos direitos fundamentais: uma teoria geral dos direitos fundamentais na perspectiva constitucional. Porto Alegre, RS: Livraria do Advogado.

SCHWABE, Jürgen, 2005. Cinquenta anos de jurisprudência do Tribunal Constitucional Federal Alemão. Tradução de Beatriz Hennig, Leonardo Martins, et al. Montevideo: Fundación Konrad-Adenauer. [Acesso em 29 março 2021]. Disponível em: [https://www.kas.de/c/document\\_library/get\\_file?uuid=cob3d47d-beba-eb55-ob11-df6c530ddf52&groupId=252038](https://www.kas.de/c/document_library/get_file?uuid=cob3d47d-beba-eb55-ob11-df6c530ddf52&groupId=252038).

PÁDUA, Luciano, 2018. Brasil deixa de receber informações de MPs estrangeiros por falta de lei de dados. Jota [em linha]. 14 agosto 2018. [Acesso em 29 março 2021]. Disponível em: <https://www.jota.info/coberturas-especiais/liberdade-de-expressao/cooperacao-juridica-dados-pessoais-14082018>.

UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho. Bruxelas, 27 abr. 2016. Jornal Oficial da União Europeia (PT), 4 maio 2016. p. L119/1-L119/88. [Acesso em 29 março 2021]. Disponível em: [https://www.cncs.gov.pt/content/files/regulamento\\_ue\\_2016-679\\_-\\_protecao\\_de\\_dados.pdf](https://www.cncs.gov.pt/content/files/regulamento_ue_2016-679_-_protecao_de_dados.pdf).

VITALE, Marco Queiroz, 2014. Control Over Personal Data, Privacy And Administrative Discretion In Europe And The USA: The Paradox Of Italian “Data Protection Authority”. *The John Marshall Journal of Information Technology & Privacy Law* [em linha]. 2014. vol. 30.