O compartilhamento de dados pessoais dos beneficiários do auxílio emergencial à luz da Lei Geral de Proteção de Dados

Sharing personal data of emergency aid beneficiaries under the General Law on Data Protection

Adriana Carla Silva de Oliveira[a]

Douglas da Silva Araújo[b,*]

RESUMO: No atual contexto da pandemia emergiu de forma exponencial um debate acerca da coleta, uso e compartilhamento de dados pessoais pelo poder público para a definição e implementação de políticas públicas emergenciais de combate ao COVID-19. Entretanto, a grande preocupação reside em como os dados pessoais e os dados pessoais sensíveis estão sendo tratados, compartilhados e armazenados pelos organismos governamentais. Recentemente, o governo federal do Brasil publicou no Portal da Transparência dados pessoais de quase 57 milhões de brasileiros que receberam auxílio emergencial, benefício instituído pela Lei de nº 13.982/2020. O objetivo da presente pesquisa é caracterizar a natureza dos dados pessoais dos beneficiários do auxílio emergencial divulgados pelo Portal da Transparência do governo federal, bem como analisar a conduta de compartilhamento desses dados entre os órgãos do governo à luz da política de proteção de dados pessoais, instituída pela Lei nº 13.709/2018, denominada em Lei Geral de Proteção de Dados (LGPD). Ao final, constatou-se que os dados divulgados têm natureza sigilosa, conforme disposição legal, e para que sejam considerados públicos se faziam necessárias medidas técnicas de anonimização e de segurança da informação para garantia mínima do padrão de privacidade quando lançadas em portais de transparência.

Palavras-chave: COVID-19; Dados Pessoais; Auxílio Emergencial; Anonimização; Lei Geral de Proteção de Dados.

ABSTRACT: In the current context of the pandemic, a debate has emerged exponentially about the collection, use and sharing of personal data by the Government for the definition and implementation of emergency public policies to combat COVID-19. However, a major concern is how personal data and sensitive personal data are being treated, shared and stored by government agencies. Recently, the federal government of Brazil published on the Transparency Portal personal data of almost 57 million Brazilians who received emergency aid, a benefit established by Law No. 13.982 / 2020. The purpose of this research is to characterize the nature of the beneficiaries' personal data emergency assistance through the federal government's Transparency Portal, as well as analyzing the conduct of data sharing between government agencies in the light of the personal data protection policy, instituted by Law No. 13,709 / 2018, referred to as the General Law on Data Protection (LGPD). Finally, it was found that the data disclosed is of a confidential nature, legal provision, and in order to be considered public, technical measures of anonymization and information security were necessary to ensure minimum privacy standards when posted on transparency portals.

Keywords: COVID-19; Personal Data; Emergency Assistance; Anonymization; General Law on Data Protection.

[a] Universidade Federal do Rio Grande do Norte, Natal, RN, Brasil.

[b] Universidade Potiguar, Natal, RN, Brasil.

* Correspondência para/*Correspondence to*: Douglas da Silva Araújo. E-mail: douglasaraujojp@gmail.com.

Recebido em/*Received*: 15/08/2020; Aprovado em/*Approved*: 13/12/2020.

INTRODUÇÃO

O ano de 2020 está sendo marcado por uma crise mundial que traz à tona a reflexão em torno dos acontecimentos emergidos no epicentro da pandemia, a pesquisa científica colaborativa no arcabouço da Ciência e as ações governamentais se uniram numa tentativa de encontrar possíveis soluções para este fenômeno global.

Nesse sentido, a pandemia nos trouxe para reflexão deste artigo duas abordagens: a primeira relacionada à gravidade e necessidade de políticas públicas emergenciais de combate, monitoramento e ações integradas de saúde, e por outro lado, a coleta, o tratamento e o compartilhamento de dados pessoais e dados pessoais sensíveis para a divulgação científica acerca da pandemia do COVID-19, em especial pelos entes públicos.

Transversalmente, aponta-se que neste contexto, emergiu de forma exponencial Políticas Públicas emergenciais do governo federal, como o auxílio emergencial para a população brasileira mais carente. Soma-se a este fato que, a coleta e o uso de dados pessoais e de dados pessoais sensíveis para o estabelecimento dessas políticas emergenciais são inevitáveis, bem como a necessidade dos entes públicos em dar o máximo de transparência pública e prestação de contas à sociedade de forma proativa.

Contudo, a partir de um cenário de pandemia, cabe aos entes públicos e a iniciativa privada, garantir que tais ações sejam respaldadas em evidências científicas e técnicas quanto à necessidade e a eficiência da coleta, do tratamento, do uso, do monitoramento, do armazenamento e do compartilhamento de dados pessoais e sensíveis com menor risco à privacidade dos seus titulares e, por conseguinte do cidadão brasileiro.

Quando a Administração Pública atua no campo da privacidade e dos dados pessoais, a operação de tratamento é, sem sombra de dúvida, um ato administrativo e como tal, detém como pressuposto de validade a finalidade pública, que neste caso, está intrinsecamente relacionada ao interesse público que alicerça a operação de uso desses dados.

A própria Lei Geral de Proteção de Dados (LGPD) admite, em seu art. 7º, inciso III, o tratamento e compartilhamento de dados pessoais pela Administração Pública quando necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV da referida norma.

A partir dessas considerações, este trabalho tem por objetivo caracterizar a natureza dos dados pessoais dos beneficiários do auxílio emergencial pelo Portal da Transparência do governo federal, bem como analisar a conduta de compartilhamento desses dados entre os órgãos do governo à luz da política de proteção de dados pessoais, instituída pela Lei nº 13.709/2018, denominada em Lei Geral de Proteção de Dados (LGPD).

A ATUAÇÃO DO PODER PÚBLICO NO TRATAMENTO DE DADOS

A atividade de tratamento de dados pessoais é hoje uma realidade tanto no setor público como no setor privado, sobretudo pelo avanço das tecnologias da informação e comunicação, difundidas especialmente pelo uso maciço da rede mundial de computadores (internet), responsável por conectar pessoas, entidades, organismos, que trocam e compartilham informações diariamente.

Deve-se se ter em mente que a maneira de como se dá o tratamento de dados pessoais pode afetar diretamente o direito à privacidade de qualquer indivíduo, por isso a importância de regulação da matéria, tendo em vista que todo cidadão tem o direito de ter acesso aos seus dados pessoais, o direito de retificá-los ou excluí-los, de decidir a respeito de seu destino e finalidade (Tavares, Alvarez 2017).

Na perspectiva do tratamento de dados, a LGPD estabeleceu princípios, garantias, deveres e direitos dos cidadãos, dos prestadores de serviços e do próprio poder público, considerando que, expressamente, submeteu este último às suas diretrizes, conforme disposição contida no *caput* do seu artigo 23, o qual impõe às pessoas jurídicas de direito público a observância da finalidade pública, a persecução do interesse público, quando exercerem atividade de tratamento de dados pessoais.

O artigo 23 da LGPD ainda menciona quais são as pessoas jurídicas de direito público submetidas à lei, fazendo menção expressa ao parágrafo único do art. 1º da Lei nº 12.527/2011 (Lei de Acesso à Informação), alcançando os órgãos públicos integrantes da administração direta dos Poderes Executivo, Legislativo, incluindo as Cortes de Contas, e Judiciário e do Ministério Público, as autarquias, as fundações públicas, as empresas públicas, as sociedades de economia mista e demais entidades controladas direta ou indiretamente pela União, Estados, Distrito Federal e Municípios.

Assim, conclui-se preliminarmente que tanto a LGPD quanto a LAI se aplicam às pessoas jurídicas da administração pública direta e indireta, especialmente quando essas pessoas estiverem desempenhando atividades de tratamento de dados pessoais, que correspondem às seguintes situações: a) para o atendimento de finalidade pública; b) na persecução do interesse público; c) com o objetivo de executar as competências legais; d) para cumprir atribuições legais do serviço público.

Ademais, o uso compartilhado de dados pessoais pelo poder público deve atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios de proteção de dados pessoais da lei em estudo.

Nessa perspectiva, a segurança jurídica de respaldo à proteção dos dados pessoais e do dado pessoal sensível é uma premissa obrigatória, bem como, no compartilhamento desses dados, mesmo que revestidos de caráter público, as diretrizes principiológicas precisam ser observadas.

No atual cenário de pandemia, pode-se perceber como o compartilhamento de dados pessoais foi utilizado pelo poder público para o desenvolvimento de ações voltadas ao combate da Pandemia do COVID-19, como aconteceu com o governo de São Paulo que firmou parceria com as empresas de telefonia, no intuito de obter informações a partir de dados de geolocalização, que oportunizou o acesso a outras informações pessoais dos usuários, como a frequência de deslocamentos, as datas de cada geolocalização, além do nome e número de telefone (A proteção…, 2020).

Destarte que "o uso de dados de maneira legítima é essencial à formulação de políticas públicas e iniciativas privadas para o combate ao COVID-19. Entender como a população tem se comportado pode ajudar o poder público a antecipar demandas e alocar recursos, pessoal e medidas de contenção de forma mais eficiente" (Bioni, Zanatta, Monteiro, 2020). Contudo, a grande preocupação reside em como os dados pessoais e os dados pessoais sensíveis estão sendo tratados, compartilhados e armazenados, considerando a existência da Lei nº 13.979/2020 que determina ser "obrigatório o compartilhamento entre órgãos e entidades da administração pública federal, estadual, distrital e municipal de dados essenciais à identificação de pessoas infectadas ou com suspeita de infecção pelo coronavírus, com a finalidade exclusiva de

evitar a sua propagação", e qual a compreensão da população, do cidadão comum frente a esse volume de dados e informações científicas que estão sendo propagadas.

Antes de analisar a responsabilidade do poder público no tratamento de dados pessoais e dados pessoais sensíveis, sobretudo os dados dos beneficiários do auxílio emergencial, é importante conhecer a definição dessas categorias. Conforme o art. 5°, incisos I e II da Lei Geral de Proteção de Dados (LGPD), considera-se dado pessoal toda informação relacionada a pessoa natural identificada ou identificável, como nome completo, endereço, dados de localização, identificadores online, renda etc. Já dado pessoal sensível é todo dado sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural. Alguns casos de dados sensíveis, em especial quando se tratam de crianças e adolescentes, a lei prevê procedimentos específicos.

Salienta-se que as definições acima, caracterizam os dados pessoais e dados pessoais sensíveis no rol da LGPD e que estão totalmente relacionados com o atual compartilhamento de dados públicos.

Perceba-se que os dados pessoais sensíveis, conforme transcrito acima, são espécies de dados que podem ensejar a discriminação do seu titular, sobretudo por guardarem relação, por exemplo, com a opção sexual, opiniões políticas, informações genéticas, convicções religiosas, filosóficas ou morais, o que faz aumentar ainda mais a responsabilidade de quem os gerenciam.

Com o objetivo de proteger os dados pessoais, especialmente os sensíveis, existem técnicas de anonimização, que podem ser perfeitamente utilizadas pelo poder público, inclusive quando tais dados forem utilizados para fins de elaboração, implementação e avaliação de políticas públicas.

Além da anonimização, existem outras maneiras de proteger os dados pessoais e sensíveis, como a criptografia e tokenização (Machado, Duarte Neto, Bento Filho 2019).

Embora o poder público tenha em seu favor exceções trazidas pela própria LGPD no âmbito do tratamento dos dados pessoais, previstas dos artigos 23 ao 32, que se justificam no princípio administrativo basilar da supremacia do interesse público sobre o privado, isso não isenta gestores e agentes públicos de obrigatoriedades e responsabilidades. Sobre este ponto, interessante observação foi feita por Gonçalves (2019, p. 133):

> Ações precipitadas pela Administração Pública, apesar de muitas vezes bem-intencionadas, que visam ao atendimento dos princípios da transparência e da publicidade, também podem ferir os direitos da personalidade, uma vez que podem permitir o acesso a terceiros ou tornar públicos dados pessoais ou tornados sensíveis pelo cruzamento entre diferentes bases de dados.

Sendo assim, o uso compartilhado e a disponibilização de dados pela Administração Pública requer mecanismos e ferramentas que garantam a governança e a segurança da informação, em que dados pessoais e dados sensíveis a partir de processos de anonimização e de outras medidas técnicas possam adquirir o "*status*" de dados públicos e que, consequentemente, a proteção desses dados seja minimamente garantida.

Por fim, corroborando essa perspectiva Tasso (2019, p. 280) afirma que

> Dados pessoais ou sensíveis não perdem a natureza ou proteção legal pelo fato de integrarem bases de dados públicos. Não por outro motivo, a regra do artigo 7º, § 3º, da LGPD prescreve que o tratamento de dados pessoais cujo acesso é público deve considerar a finalidade, a boa-fé e o interesse público que justificam sua disponibilização.

Em suma, a regra é clara que a natureza dos dados pessoais e sensíveis não altera quando estes se tornam públicos, conquanto a observância aos princípios, a proporcionalidade para aferição dessa transferência e a finalidade pública devem ser observadas. Por ora, depreender dessa afirmativa enseja também o debate das próximas seções.

A NATUREZA DOS DADOS DOS BENEFICIÁRIOS DO AUXÍLIO EMERGENCIAL

O governo federal publicou no início de junho de 2020 no Portal da Transparência dados pessoais de quase 57 milhões de brasileiros que receberam auxílio emergencial, benefício instituído pela Lei de nº 13.982/2020, destinado a trabalhadores informais e de baixa renda, microempreendedores individuais e também contribuintes individuais do Instituto Nacional do Seguro Social, que tem por objetivo minimizar os efeitos sociais e econômicos da pandemia ocasionada pelo COVID-19 (Maranhão, Senhoras 2020). O ministro da Controladoria-Geral da União (CGU), Wagner Rosário, também divulgou os dados dos beneficiários do auxílio, em especial das parcelas de abril e maio, em sua página na rede social *Twitter* (Rosário 2020).

Após consulta aos *links* das listas publicadas pelo governo federal, é possível verificar que dentre as informações divulgadas estão o estado, a cidade, o número de identificação social (NIS), o CPF (seis dígitos do meio), o nome completo do beneficiário e o valor recebido do auxílio emergencial por cada cidadão.

A pretexto de viabilizar a fiscalização por parte da população, é possível verificar verdadeira lesão ao Direito à Privacidade desses indivíduos, neste caso, os cidadãos brasileiros.

Refinando esse debate, especialmente à luz da Lei Geral de Proteção de Dados, dois conceitos especiais precisam ser considerados para delimitar e entender se o governo brasileiro incorre em ilícito ao fazer essa divulgação, são eles "dados públicos" e "dados manifestamente públicos".

A princípio essas duas categorias podem até soar como sinônimas, contudo, epistemologicamente decorrem de parâmetros distintos de entendimento. Os dados públicos são exatamente aqueles encontrados nos portais estatais, diários oficiais, editais públicos, sem que necessariamente tenham sido publicizados e autorizados pelo titular. A propósito, a LGPD em seu art. 7º, §3º aduz que "o tratamento de dados pessoais cujo acesso é público deve considerar a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização".

Essa definição de dados públicos oferecida pela LGPD só será melhor entendida com a leitura conjugada do referido dispositivo com o art. 23 da mesma norma, que permite o tratamento de dados pelo poder público com objetivo de executar as competências legais e para cumprir atribuições legais do serviço público, observando a finalidade e o interesse público envolvidos, com o fornecimento de informações claras sobre a previsão legal, os procedimentos e as práticas utilizadas para execução dessas atividades.

A interpretação sistemática dos dispositivos da LGPD permite, portanto, definir dados públicos como aqueles cuja publicidade das informações se justificam no interesse público, detendo finalidade vinculada a previsão legal autorizativa, sendo irrelevante o consentimento do titular, ressalvadas as hipóteses de abusos e desvirtuamento dessa finalidade.

Buscando definir dados públicos, Bruno Bioni (2019) alude que para serem considerados públicos é necessária uma análise do contexto pelo qual tais dados são publicamente acessíveis, ou seja, saber o motivo, a razão da publicização da informação, o que o autor denomina de "privacidade contextual", sustentando que, o que vai definir se o tratamento é ilegal ou não é a compatibilidade dessa publicização com a finalidade e o interesse pelo quais tais dados foram considerados de acesso público.

Já os "dados manifestamente públicos" guardam estrita relação com o consentimento prévio, muito embora num segundo momento ele seja dispensável. Explique-se melhor, malgrado esses dados possam estar disponíveis em ambiente público, como em redes sociais e sites da *internet*, essa disponibilização decorreu da vontade do titular, que, necessariamente, vincula-se ao motivo da presença dos dados nesses ambientes. Empresas privadas ou até mesmo entidades da administração pública que coletarem ou se utilizarem desses dados poderão ser submetidas ao ônus da comprovação do consentimento (art. 8º, § 2º c/c art. 42, § 2º, da LGPD) e o uso deles estará limitado à finalidade da autorização inicial dada pelo titular. Um exemplo é a reprodução de dados da Plataforma Lattes (http://lattes.cnpq.br/) pelo site Escavador (https://www.escavador.com/), que divulga informações oriundas de fontes públicas, como publicações científicas, oferecendo uma espécie de serviço de indexação que auxilia na divulgação e facilita a busca por parte dos interessados, sem alterar a finalidade pela qual foram publicizados.

Contudo, a previsão da LGPD sobre os dados manifestamente públicos é bem controvertida, especialmente pela redação dada ao § 4º, do artigo 7º, *in verbis*: "é dispensada a exigência do consentimento previsto no *caput* deste artigo para os dados tornados manifestamente públicos pelo titular, resguardados os direitos do titular e os princípios previstos nesta Lei".

A princípio, pela dicção do dispositivo, é possível concluir que os dados manifestamente públicos estão dentre as hipóteses de dispensa do consentimento, porém, mais uma vez, é necessária uma interpretação sistemática da norma, principalmente da parte final, para delimitar o conceito dessa categoria. A ressalva do artigo impõe a observância dos direitos do titular, dentre eles o consentimento. Entender de forma diversa, possibilitaria a autorização da coleta, do compartilhamento, ou seja, do tratamento desses dados sem qualquer vinculação à vontade do titular ou a presença do interesse público que justificasse a dispensa do consentimento, indo de encontro com a finalidade da própria norma. Sem dúvida, foi uma incongruência do legislador.

Corroborando essa perspectiva, Oliva e Viégas (2019) afirmam que o art. 7º, § 4º, da LGPD dispensa a exigência de consentimento em relação aos "dados tornados manifestamente públicos pelo titular", contudo, carecem de definição os contornos a serem outorgados à autorização de tratamento dos dados tornados manifestamente públicos pelo titular, mas é certo que, mesmo nesses casos, o tratamento de tais dados continua sujeito ao respeito aos direitos do titular.

Por sua vez, Bioni (2019) também relaciona a "privacidade contextual" aos dados manifestamente públicos, no entanto, reforça a necessidade de haver compatibilidade

entre o seu uso por terceiros e as circunstâncias pelas quais tal dado foi tornado público pelo titular. Embora esses tipos de dados sejam considerados públicos, não deixam de ser pessoais, sendo necessário considerar sempre a finalidade da circulação e o que justifica sua disponibilização (Tepedino, Teffé 2019).

Perceba-se uma diferença básica entre dados públicos e dados manifestamente públicos. Os primeiros estarão caracterizados a partir do interesse público presente na sua divulgação, cuja finalidade do tratamento pressupõe uma permissão normativa, prescindindo totalmente do consentimento por parte do titular. Já a segunda categoria, dados manifestamente públicos, vincula o uso desses dados por terceiros à vontade prévia do titular no momento que disponibiliza esses dados em ambientes de acesso público, mesmo que num segundo momento esse consentimento seja dispensado.

A título de exemplo, enquanto dados públicos, a divulgação de salários de servidores em portais de transparência justifica-se no direito da população em saber como os recursos públicos estão sendo empregados, incluídas as remunerações pagas aos ocupantes de cargos públicos, pois decorrentes do pagamento de impostos, representando um verdadeiro exercício de cidadania pela população. O interesse público resta perfeitamente evidenciado nessa situação. Diferentemente ocorre quando alguma empresa ou entidade pública se apropria de dados de usuários disponíveis em ambientes ou plataformas de acesso público, ou seja, manifestamente públicos, como as redes sociais, repositórios institucionais, e dão destinação diversa daquela informada no momento da coleta ou da inserção desses dados, desvirtuando sua finalidade.

É válido também ressaltar que dados públicos guarda estrita relação com o conceito de dados abertos, adquirindo essa característica quando são disponibilizados de forma irrestrita. Para Oliveira (2016, p. 53) "para que os dados assumam o *status* de aberto, mesmo que produzidos em diversos contextos (científicos, governamentais, institucionais, privados e públicos) é condicionante que estejam acessíveis gratuitamente, com permissão legal ou licenciados para uso, cópia, download, visualização, análise,uso, reuso e na forma digital".

Conforme o Manual de Dados Abertos Governamentais (2017, p. 11), confeccionado pelo governo do Rio Grande do Sul, "todo dado público tem vocação para ser aberto. Por dado público entende-se aquele que não está sujeito a limitações válidas de privacidade, segurança, controle de acesso ou outros privilégios, desde que transparente, bem justificado e regulado por estatutos".

A publicação dos dados públicos em formato aberto está prevista na Lei de acesso à informação - Lai (Lei nº 12.527, de 18 de novembro de 2011), e parte do pressuposto que a informação produzida pela atividade estatal pertence à sociedade, e a ela deve estar acessível (Manual 2017).

Segundo o Guia de Dados Abertos (Pires 2015, p. 11) "todo dado que é público deve ser aberto, mas nem todo dado é público". Cabe ao governo avaliar as possibilidades de abertura de dados, o que implica delimitar, de maneira clara e transparente, quais dados armazenados pelos órgãos e entidades são passíveis de acesso e quais não são (Possamai, Souza 2017).

Nesse prisma, dados públicos devem ser abertos, estes caracterizados pela livre e gratuita possibilidade de acesso, utilização, modificação e compartilhamento, estando isentos de direitos autorais. Contudo, nem todo dado governamental é público e, quando não o é, não poderá se "aberto", a exemplo dos dados sigilosos, como é o caso dos dados dos beneficiários do auxílio emergencial, conforme se verá mais à frente.

Outra questão que também merece análise no contexto dessa divulgação de informações pelo governo federal é de como se deu o compartilhamento dos dados dessas pessoas entre organismos estatais, o Cadastro Único, vinculado ao Ministério do Desenvolvimento Social e o Portal da Transparência, ligado ao Ministério da Cidadania. Sobre esse assunto, válido transcrever o que diz a Lei Geral em seu artigo 26:

> Art. 26. O uso compartilhado de dados pessoais pelo Poder Público deve atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios de proteção de dados pessoais elencados no art. 6º desta Lei.
> § 1º É vedado ao Poder Público transferir a entidades privadas dados pessoais constantes de bases de dados a que tenha acesso, exceto:
> I - em casos de execução descentralizada de atividade pública que exija a transferência, exclusivamente para esse fim específico e determinado, observado o disposto na Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação);
> II - (VETADO);
> III - nos casos em que os dados forem acessíveis publicamente, observadas as disposições desta Lei.
> IV - quando houver previsão legal ou a transferência for respaldada em contratos, convênios ou instrumentos congêneres; ou
> V - na hipótese de a transferência dos dados objetivar exclusivamente a prevenção de fraudes e irregularidades, ou proteger e resguardar a segurança e a integridade do titular dos dados, desde que vedado o tratamento para outras finalidades.
> § 2º Os contratos e convênios de que trata o § 1º deste artigo deverão ser comunicados à autoridade nacional.

Pela dicção da regra, é possível concluir que o compartilhamento entre os órgãos que compõem a Administração Pública estará atrelado a finalidade da política pública que justifique essa ação, observando os princípios gerais insculpidos pela lei, além da necessidade de haver previsão legal ou contratual que subsidie esse compartilhamento.

Além da LGPD, o governo federal editou, em 09 de outubro de 2019, o Decreto 10.046, que estabelece a política de compartilhamento de dados no âmbito da administração pública federal. Para a norma, a política de compartilhamento de dados terá como finalidade simplificar a oferta de serviços públicos, orientar e otimizar a formulação, a implementação, a avaliação e o monitoramento de políticas públicas, possibilitar a análise das condições de acesso e manutenção de benefícios sociais e fiscais, promover a melhoria da qualidade e da fidedignidade dos dados custodiados pela administração pública federal e aumentar a qualidade e a eficiência das operações internas da administração pública federal.

Esse compartilhamento de dados entre as pessoas jurídicas de direito público impõe ao Poder Público a obrigação de ser ainda mais transparente, "o que envolve a publicidade quanto à motivação, ao uso e à finalidade para a qual os dados foram coletados, conferindo maior controle ao cidadão sobre as ações adotadas, sendo, também, uma forma de accountability" (Gonçalves 2019, p.114).

É evidente que tais premissas não foram observadas pelo governo federal ao compartilhar os dados dos beneficiários do auxílio emergencial no Portal da Transparência. Primeiro porque os dados constantes em cadastros sociais, como o Cadastro Único, não possuem caráter público. Conforme preleciona o art. 8º do

Decreto nº 6.135/2007, que dispõe sobre o Cadastro Único para Programas Sociais do governo federal, "os dados de identificação das famílias do CadÚnico são sigilosos e somente poderão ser utilizados para as seguintes finalidades: I - formulação e gestão de políticas públicas; e II - realização de estudos e pesquisas". Segundo porque inexiste liame entre a disponibilização consciente desses dados no CadÚnico e a intenção que lhe fora atribuída, justificada num suposto viés fiscalizatório que ensejou a "transparência" das informações, diversa do propósito e da finalidade do cadastro (Brasil, 2017).

Ademais, a divulgação dos dados nos moldes em que foi realizada não encontra justificativa no interesse público, nem havia política pública que embasasse o compartilhamento dessas informações entre os órgãos do governo e muito menos foi utilizada técnica de anonimização que impedisse a associação dos dados ao seu titular.

O uso de dados de maneira legítima é essencial à formulação de políticas públicas e iniciativas privadas para o combate ao COVID-19. Assim, revela-se essencial a adoção de medidas técnicas robustas de anonimização e proibição de monetização de dados sensíveis ou uso para quaisquer outras finalidades além das necessárias para o combate à pandemia (Bioni, Zanatta, Monteiro, 2020).

CONSIDERAÇÕES FINAIS

Na esteira desse debate, pode-se concluir que a conduta do governo federal em disponibilizar dados pessoais de brasileiros que receberam auxílio emergencial no Portal da Transparência violou os direitos à privacidade e intimidade dessas pessoas, especialmente pela natureza sigilosa que esses dados detêm.

Na divulgação das informações pessoais desses beneficiários (cidade, estado, número de identificação social, nome completo, valor recebido) não foram observadas medidas técnicas e administrativas aptas a garantir o sigilo de dados e sua anonimização. Ademais, é possível também concluir não estar presente interesse público legítimo a justificar tão ampla publicização de dados.

A decisão em divulgar tais dados violou garantias constitucionais, especialmente aquelas previstas no art. 5º, X e XII, da Constituição Federal, sem a devida observância aos princípios norteadores da Lei Geral de Proteção de Dados, sobretudo a finalidade, a segurança, a necessidade e a adequação, o que poderia ter sido suplantado com a utilização de técnicas de anonimização ou mesmo se considerados de forma agregada ou estatística.

A honra, a privacidade, a intimidade são direitos inerentes à condição de pessoa humana e, num estado democrático de direito, esses direitos estão acobertados pela tutela judicial. Da ofensa aos direitos da personalidade, incluídos o da privacidade e da intimidade, emerge a possibilidade da indenização pelos danos sofridos, conforme o já mencionado artigo 5º, inciso X, da Carta Política.

Caso fosse a vontade do governo de fiscalizar e investigar eventuais ilícitos no recebimento desse auxílio, deveria acionar os órgãos de controle (Controladoria-Geral da União, Ministério da Cidadania e Receita Federal) (Richter 2020) que, individualmente e usando dos instrumentos próprios, buscarão reaver eventuais valores auferidos indevidamente.

Ao incorrer em ilícito contra a privacidade dos cidadãos brasileiros que receberam o auxílio, surge para estas a possibilidade de ingressar com a ação competente contra o governo federal (União) por eventuais danos sofridos com essa publicização e

exposição indevidas. Após divulgação no Portal da Transparência, em diversas cidades brasileiras, por exemplo, foram disseminadas notícias contra servidores públicos que receberam o auxílio irregular de forma pejorativa e devassando a intimidade dessas pessoas, boa parte dessas notícias de cunho político-partidário. Neste caso, os fins não justificam os meios.

Nessa perspectiva, surge um grande desafio aos gestores públicos que é o de conciliar a transparência que deve reger os atos da administração pública e, ao mesmo tempo, observar o regime jurídico de proteção de dados inaugurado pela LGPD. Muito embora possa se enxergar uma dicotomia entre esses temas, um alinhamento entre a Autoridade Nacional de Proteção de Dados (ANPD) e os órgãos de controle, a exemplo da Controladoria-Geral da União, será crucial para conciliação do direito à proteção de dados com a transparência pública, a partir da elaboração de normas que detalhem o regramento, limites e alcance da LGPD, sobretudo no campo dos dados públicos, dados abertos e governamentais.

REFERÊNCIAS

A PROTEÇÃO de dados pessoais em época de pandemia, 2020. *UFJF Notícias*, 28 de maio de 2020. Disponível em: https://www2.ufjf.br/noticias/2020/05/28/a-protecao-de-dados-pessoais-em-epoca-de-pandemia/. Acesso em: 07 jul. 2020.

BIONI, B. R. *Proteção de dados pessoais:* a função e os limites do consentimento. Rio de Janeiro: Forense, 2019.

BIONI, Bruno; ZANATTA, Rafael; MONTEIRO, Renato; RIELLI, Mariana. *Privacidade e pandemia:* recomendações para o uso legítimo de dados no combate à COVID-19. Conciliando o combate à COVID-19 com o uso legítimo de dados pessoais e o respeito aos direitos fundamentais. São Paulo: Data Privacy Brasil, 2020. Disponível em: . https://www.dataprivacybr.org/wp-content/uploads/2020/04/ relatorio_privacidade_ e_pandemia_final.pdf. Acesso em: 01 ago. 2020.

BRASIL. *Decreto n. 6.135, de 26 de junho de 2007.* 2007. Disponível em: http://www.planalto.gov.br . Acesso em: 05 jul. 2020

BRASIL. *Decreto n. 10.046, de 9 de outubro de 2019*. 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Decreto/D10046.htm. Acesso em: 25 jul. 2019.

BRASIL. *Lei nº 12.527, de 18 de novembro de 2011*. 2011. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm

BRASIL. *Lei n. 13.709, de 14 de agosto de 2018*. 2018. Disponível em: http://www.planalto.gov.br. Acesso em: 25 jul. 2019.

GONÇALVES, Tânia Carolina Nunes Machado. *Gestão de dados pessoais e sensíveis pela Administração Pública Federal:* desafios, modelos e principais impactos com a nova lei. 2019. Dissertação (Mestrado em Direito) - Centro Universitário de Brasília, 2019.

MACHADO, J. C.; DUARTE NETO, E. R.; BENTO FILHO, M. E. *Técnicas de privacidade de dados de localização* (minicurso). 2019. Disponível em: http://sbbd.org.br/2019/wp-

content/uploads/sites/6/2019/10/Apresentacao_Minicurso_1_Privacidade.pdf. Acesso em: 12 jul. 2020.

MANUAL de dados abertos governamentais, 2017. Disponível em: https://dados.rs.gov.br/about. Acesso em: 25 jul. 2020.

MARANHÃO, R. A.; SENHORAS, E. M. Orçamento de Guerra no enfrentamento à COVID-19: entre manobras parlamentares e batalhas políticas. *Boletim de Conjuntura (BOCA)* v. 2, n. 6, 2020. Disponível em: https://revista.ufrr.br/boca/article/view/OrcamentoGuerra. Acesso em: 27 jul. 2020.

OLIVA, M. D.; VIÉGAS, F. A, Tratamento de dados para concessão de crédito. *In:* FRAZÃO, A.; TEPEDINO, G.; OLIVA, M. D. (orgs.). *Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro.* São Paulo: Thomson Reuters Brasil, 2019.

OLIVEIRA, Adriana Carla Silva de. *Desvendando a autoralidade colaborativa na e-science sob a ótica dos direitos de propriedade intelectual.* 2016. Tese (Doutorado em Ciência da Informação) - Universidade Federal da Paraíba, 2016.

PIRES, Marco Túlio. *Guia de Dados Abertos*: Governo do Estado de São Paulo. 2015. Disponível em: https://nic.br/media/docs/publicacoes/13/Guia_Dados_Abertos.pdf. Acesso em: 20 jul. 2020.

POSSAMAI, Ana Júlia. SOUZA, Vitoria Gonzatti de. Transparência e dados abertos no governo federal: possibilidades e desafios a partir da lei de acesso à informação. *Anais do Encontro Nacional de Ensino e Pesquisa do Campo de Públicas*, v. 2, n. 2, 2017. Disponível em: http://www.anepcp.org.br/acp/anaisenepcp/20180723152454_35_Transparencia_e_dados_abertos_Ana_Possamai.pdf. Acesso em: 01 ago. 2020.

RICHTER, A. Cidadania e Receita ampliam fiscalização do auxílio emergencial. *Agência Brasil,* 09 jul. 2020. Disponível em: https://agenciabrasil.ebc.com.br. Acesso em: 01 jul. 2020.

ROSÁRIO, W. Beneficiários do auxílio emergencial. *Twitter WRosarioCGU.* 2020. Disponível em: https://twitter.com/WRosarioCGU. Acesso em: 12 jul. 2020.

TASSO, Fernando Antonio. Do tratamento de dados pessoais pelo poder público. *In:* MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (coord.). *LGPD:* Lei Geral de Proteção de Dados: comentada. São Paulo: Revista dos Tribunais, 2019.

TAVARES, Letícia Antunes. ALVAREZ, Bruna Acosta. Da proteção dos dados pessoais: uma análise comparada dos modelos de regulação da Europa, dos Estados Unidos da América e do Brasil. *In:* BRASIL e EUA: temas de direito comparado. São Paulo: Escola Paulista da Magistratura, 2017.

TEPEDINO, G.; TEFFÉ, C. S. Consentimento e proteção de dados pessoais na LGPD. *In:* FRAZÃO, A.; TEPEDINO, G.; OLIVA, M. D. (orgs.). *Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro.* São Paulo: Thomson Reuters Brasil, 2019.