CALAMIDADE PÚBLICA E DIREITOS FUNDAMENTAIS: A PANDEMIA DE COVID-19 E A PROTEÇÃO DE DADOS PESSOAIS PELA LGPD

Henrique da Rosa Ziesemer[1]
Luiz Fernando Rossetti Borges[2]

Recebido em 20/09/2022
Aceito em 11/11/2022

RESUMO
A proteção dos dados pessoais ganha relevo em período de pandemia de Covid-19, porquanto podem ser utilizados no seu enfrentamento, especialmente na elaboração de políticas públicas. Busca-se com este estudo argumentar em torno da proteção de direitos fundamentais, notadamente da privacidade e da intimidade, em relação aos quais se lançam discussões pela urgência pandêmica. Como problema do presente trabalho, questiona-se se as medidas restritivas de liberdades, aplicadas no contexto da pandemia de Covid-19, poderiam representar ameaças à proteção de dados pessoais, bem como quais seriam os critérios e os mecanismos que poderiam ser aplicados, com o fito de compatibilizar a proteção dos direitos fundamentais envolvidos. No que concerne à hipótese, afirma-se que, diante dos riscos implicados na restrição de medidas restritivas excessivas, devem ser estabelecidos limites éticos, técnicos e jurídicos (processuais e materiais) para proteção dos (geo)dados pessoais, de forma a serem observados os direitos fundamentais da intimidade e da privacidade, inclusive em período pandêmico, não obstante a necessidade de aprimoramento legislativo. Assim, utilizando-se do método dedutivo, e da pesquisa bibliográfica, documental e jurisprudencial, em um primeiro momento objetiva-se abordar os documentos internacionais e as leis nacionais atinentes à proteção de dados, inclusive da Medida Provisória 954/2020, que autorizava o compartilhamento de dados entre empresas e o Estado. Depois, pretende-se discorrer sobre os direitos fundamentais que são vulnerados com o compartilhamento sem orientação em critérios seguros, nos planos axiológicos e normativos, notadamente da União Europeia, bem como a exigência de normas técnicas e jurídicas para conferir segurança. Por fim, abordam-se a defesa em juízo dos dados pessoais e sua natureza como direito coletivo, não obstante a urgência do aprimoramento legislativo.

PALAVRAS CHAVE: Proteção de dados pessoais; Dados de geolocalização; Direitos fundamentais; Pandemia.

PUBLIC CALAMITY AND FUNDAMENTAL RIGHTS: THE COVID-19 PANDEMIC

[1] Promotor de Justiça do Ministério Público do Estado de Santa Catarina desde 2004. Graduado em Direito pela Universidade do Vale do Itajaí. Doutor em Ciência Jurídica (UNIVALI). Mestre em Ciência Jurídica (UNIVALI). Especialista em Direito Processual Penal. Especialista em Direito Administrativo. E-mail: henry-sc@uol.com.br. ORCID: https://orcid.org/0000-0001-6463-5222.

[2] Mestre em Direito pela Universidade Federal de Santa Catarina (UFSC), na área de Direito Internacional e Sustentabilidade (2021). Especialista em Direito e Processo Penal pela UNIVALI (2014) e pela ABDCONST (2019). Graduado em Direito pela UFSC (2012). Pesquisador do Grupo de Pesquisa em Direito Ambiental e Ecologia Política na Sociedade de Risco/GPDA (2017-atual) e do Grupo de Pesquisa Poder, Controle e Dano/GPPCDS (2020-atual). Autor de diversos artigos jurídicos na área de Direito Ambiental e Criminologia. Advogado. E-mail: luizrossettiborges@gmail.com. ORCID: https://orcid.org/0000-0001-6922-1635.

AND THE PROTECTION OF PERSONAL DATA BY LGPD

ABSTRACT
Personal geodata is becoming more important during the covid-19 pandemic because it can be used in public policy-making to address it. The study seeks to argue for the protection of fundamental rights, notably privacy and intimacy, threatened by the pandemic urgency. Based on the deductive method, bibliographic and documentary research, the study shows that the legislation on personal data, the general data protection law, already in full force, has a range of mechanisms for the protection of personal data, notwithstanding the individual and collective protection that already exists for the protection of individual liberties. Thus, using the bibliographic, documental and jurisprudential method, the international documents and national laws pertaining to data protection are initially dealt with, including medida provisória 954/2020, which authorizes data sharing between companies and the state. Then, the fundamental rights that are violated by sharing without guidance in safe criteria are discussed, in axiological and normative plans, especially from the european union, as well as the requirement of technical and legal standards to confer security. Finally, the defense of personal data in court and its nature as a collective right are addressed, notwithstanding the urgency of legislative improvement.

Keywords: Protection of personal data; Personal geodata; Fundamental rights; Pandemic.

1 INTRODUÇÃO

A sociedade contemporânea é marcada pela informação, pelo compartilhamento e armazenamento de dados, pela internet das coisas (IoT – *Internet of Things*), e outras tantas tecnologias cuja importância ganha cada vez mais espaço na vida moderna. Ao mesmo tempo, a preocupação com a privacidade e com a intimidade também cresce.

Os dados pessoais da população em geral estão armazenados em uma plêiade de bancos de dados pertencentes a empresas de todo gênero, de concessionários de serviços públicos a lojas de departamentos; de escritórios de advocacia a cartórios; de estabelecimentos bancários a empresas que funcionam *online.* Se de um lado o desenvolvimento dos negócios impulsionou o crescimento desses bancos de dados, de outro lado surgiu a preocupação com a proteção desses mesmos dados relacionados à individualidade dos cidadãos.

A pandemia acrescenta mais um elemento a ser trabalhado, visto que as medidas de restrição de liberdade individual foram e continuam sendo adotadas em todo o mundo para frear a transmissão do vírus. O compartilhamento de dados pessoais de geolocalização para elaboração de políticas públicas no cenário pandêmico é uma das interfaces dessas novas restrições pessoais.

Diante disso, emerge o contributo de Giorgio Agamben (2020a; 2020b) na teoria dos

direitos fundamentais, o qual adverte sobre os riscos à democracia que as medidas de vigilância e restritivas de mobilidade, indicadas no combate à pandemia de Covid-19, poderiam causar, em decorrência dos poderes excessivos atribuídos ao Estado.

Por outro lado, Aragão (2020) visualiza a possibilidade de serem estabelecidos mecanismos para diminuir o risco de restrição abusiva aos direitos fundamentais. De fato, como pondera Alexy (2015, p. 281), a "norma somente pode ser uma restrição a um direito fundamental se ela for compatível com a Constituição". Nesse cenário, também são debatidos os fundamentos de julgados judiciais sobre o acesso de dados pessoais a pretexto de segurança.

Importante destacar que um aspecto inovador em relação ao tema de proteção de dados pessoais e direitos fundamentais reside, do ponto de vista transnacional, no fato de que o mundo atravessa um problema de saúde pública comum, de modo a exigir uma maior interpretação e integração entre os direitos fundamentais, a contemplar sua proteção, e, igualmente, propiciar um eficiente combate à pandemia, uma vez que seu enfrentamento pode colocar em aparente colisão, direitos fundamentais, como saúde, privacidade e intimidade.

Mais recentemente a Lei Geral de Proteção de Dados Pessoais (BRASIL, 2018) entrou em plena vigência, sendo premente discutir os contornos e limites da proteção de direitos fundamentais atinentes à intimidade e à privacidade dos indivíduos em sociedade em tempo de pandemia de Covid-19. É de se mencionar também que o Congresso Nacional atualmente debate a Proposta de Emenda à Constituição n. 17/2019 (BRASIL, 2019), com o objetivo de tornar a proteção de dados pessoais um direito fundamental, o que reforça a conexão entre o Estado e a preocupação com direitos fundamentais, especialmente em situações particulares como a pandemia de Covid-19. Por sua vez, em uma Europa que também passa pela mesma situação pandêmica, o Regulamento 2016/679 do Parlamento Europeu e do Conselho da União Europeia (UNIÃO EUROPEIA, 2016) já considera o tratamento de dados pessoais um direito fundamental, havendo uma progressiva adequação nas legislações dos países-membros.

Desta forma, poder-se-ia considerar que o combate à pandemia, de alguma forma, representaria ameaça à proteção de dados pessoais? De que forma os direitos fundamentais envolvidos poderiam ser compatibilizados?

Como hipótese deste trabalho, afirma-se que devem ser estabelecidos limites éticos, técnicos e jurídicos (processuais e materiais) para proteção dos (geo)dados pessoais, de forma a serem observados os direitos fundamentais da intimidade e da privacidade, inclusive em período pandêmico.

A partir do método dedutivo, o método de procedimento monográfico e as técnicas de pesquisa bibliográfica e documental, discutem-se as questões normativas e principiológicas

atinentes à proteção dos dados pessoais e as medidas tomadas para controle e monitoramento por geolocalização na pandemia de Covid-19, principalmente à vista dos aplicativos móveis que permitem o compartilhamento de dados pessoais e de geolocalização de seus usuários.

2 A DEFESA INTERNACIONAL E NACIONAL DOS DADOS PESSOAIS

Há um mosaico de documentos internacionais que se avolumaram nas últimas décadas sobre a proteção de dados pessoais e que influenciaram a normativa brasileira, que percorre desde o âmbito de organismos internacionais até as diretivas da Comunidade Europeia.

A proteção de dados pessoais remonta, ao menos, da *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (OCDE, 1980), assinado em 1980 pelos países membros da OCDE (Organização para a Cooperação e Desenvolvimento Econômico), cujas diretrizes tinham o fito de impedir a violação de direitos fundamentais, o armazenamento ilegal de dados pessoais, o armazenamento de dados pessoais imprecisos e o abuso ou a divulgação não autorizada de tais dados.

Partindo da ideia de que o fluxo de dados pessoais já havia aumentado consideravelmente entre os países-membros do referido organismo internacional e que a introdução de novas tecnologias iria fazer esse fluxo recrudescer ainda mais, foram harmonizadas legislações internas já existentes, ao mesmo tempo que se passou a considerar os dados pessoais um direito humano, a merecer a proteção legislativa.

No âmbito da Comunidade Europeia, o Parlamento Europeu aprovou, imediatamente no ano de 1981, a Convenção do Conselho da Europa 108/1981 (UNIÃO EUROPEIA, 1981), denominada *Convenção para a Proteção de Indivíduos com Relação ao Processamento Automático de Dados Pessoais*, um documento vinculativo aos países-membros para proteger o indivíduo de abusos na coleta e armazenamento de dados pessoais, principalmente no fluxo transfronteiriço. Não obstante, proibiu-se a coleta e o armazenamento de dados pessoais sensíveis – definidos como aqueles que dizem respeito a raça, política, saúde, religião, vida sexual, antecedentes criminais, etc. – sem salvaguardas legais. O Parlamento Europeu e o Conselho, em continuidade, emitiu a Diretiva 95/46/CE (UNIÃO EUROPEIA, 1995), relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

Em análise retrospectiva, Doneda (2011) considera que:

> O ponto fixo de referência nesse processo é que, entre os novos prismas para enquadrar a questão, mantém-se uma constante referência objetiva a uma disciplina para os dados pessoais, que manteve o nexo de continuidade com a disciplina da

> privacidade, da qual é uma espécie de herdeira, atualizando-a e impondo características próprias.

Nesse mesmo prisma, em 2016, com o Regulamento 2016/679 (UNIÃO EUROPEIA, 2016) do Parlamento Europeu e do Conselho da Europa, a Comunidade Europeia traçou medidas preventivas, investigativas, de detecção e repressão de infrações penais relacionadas aos dados pessoais, sem impedir a livre circulação desses dados. A principal diferença do Regulamento para a Diretiva anterior, segundo Tateoki (2019, p. 102), está na força vinculante do Regulamento para os Estados-membros, enquanto que a Diretiva apenas impunha que os mesmos criassem normas de proteção de dados, podendo ou não as seguir.

É importante notar a influência que as diretrizes da OCDE na nascente legislação consumerista brasileira. As primeiras diretrizes da OCDE e do Código de Defesa do Consumidor se estabeleceram em um momento que as bases de dados e a troca de informações eram acentuadamente inferiores ao atual, quando "[...] as organizações coletavam dados de indivíduos, armazenavam esses dados em um computador e, em seguida, tomavam decisões e usos determinísticos sobre o indivíduo com base nesses dados" (2014, CATE et al, tradução livre).

Na busca de atualização das diretrizes de proteção de dados no âmbito da OCDE, trinta anos após a sua aprovação, foi designado um grupo de especialistas para reexaminar a matéria, os quais consideraram os seguintes fatores a serem enfrentados quanto à proteção de dados: o volume de dados pessoais coletados, usados e armazenados; a variedade de informações obtidas a partir desses dados; o valor dos benefícios sociais e econômicos viabilizados pelas novas tecnologias e uso de dados de forma responsável; a extensão de ameaças à privacidade; o número de atores capazes de colocar em risco a privacidade ou protegê-la; a frequência e a complexidade das interações envolvendo dados pessoais que se espera que indivíduos entendam e negociem; e a disponibilidade global de dados pessoais, suportada por redes e plataformas de comunicação que permitem fluxos de dados contínuos e multipontos (2014, CATE et al).

Veja-se que as primeiras diretrizes foram estabelecidas por uma organização internacional fundada para estimular o progresso econômico e o comércio mundial. Atualmente, "[os] dados são o novo petróleo", nos dizeres do CEO da Mastercard, Ajay Banga (JULIO, 2019), mas "a diferença é que o petróleo vai acabar um dia. Os dados, não". Isso decorre, segundo o executivo, pela popularização da *internet*, da era do *streaming* e da *internet* das coisas, a qual conecta as pessoas a toda uma série de aparelhos, em escala universal.

O avanço das diretrizes de proteção de dados, principalmente da Comunidade Europeia, influenciou uma série de outros países a tratar da proteção de dados pessoais mais

especificamente, notadamente nas principais economias do mundo, como o Brasil.

Assim, não obstante o amparo constitucional da intimidade, que confere a ideia de segurança pessoal e jurídica, o Brasil incorporou o tratamento da proteção de dados pessoais na Seção VI do Código de Defesa do Consumidor (BRASIL, Lei n. 8.078/1990), garantindo o acesso do consumidor aos cadastros, fichas, registros e dados pessoais e de consumo arquivados; o direito da clareza e fidedignidade das informações; a prescrição de informações negativas; o direito de ser comunicado quando da abertura de cadastro; entre outros.

No cenário de proteção de dados pessoais, foram editadas leis estabelecendo direitos e garantias na legislação infraconstitucional para eventual restrição de direitos fundamentais relacionados a dados pessoais, como (i) a Lei n. 9.296/1996 (BRASIL, 1996), que regulamenta a interceptação telefônica; (ii) a Lei Complementar n. 105/2001 (BRASIL, 2001), que trata sobre o sigilo das operações de instituições financeiras; e (iii) a Lei n. 12.965/2014 (BRASIL, 2014), conhecida como Marco Civil da Internet.

A Lei n. 13.709/2018 (BRASIL, 2018), também conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD) entrou plena vigência no final de 2020, quando foi rejeitado um dispositivo da Medida Provisória 959/2020 (BRASIL, 2020a) que buscava um novo adiamento para maio de 2021. Inspirada na legislação europeia, a LGPD é desafiada a proteger dados pessoais dos cidadãos, frente à calamidade e exceção pandêmicas.

2.1 Os direitos fundamentais frente ao compartilhamento de dados pessoais de geolocalização

Necessário, antes de tudo, estabelecer diferenças entre intimidade e privacidade. A primeira é absolutamente pessoal e diz respeito ao modo de ser de determinada pessoa. Na intimidade se revelam gostos, desejos, sentimentos e sensações. Na privacidade, por sua vez, há uma escolha (que pode ser legal ou pessoal) em que o interessado escolhe quais informações deseja difundir.

A intimidade (por extensão, a privacidade), a vida privada, a honra e a imagem são invioláveis, conforme preceitua a Constituição da República (BRASIL, 1988), a qual assegura a indenização pelos danos decorrentes do desrespeito a esses direitos.

Os direitos fundamentais à intimidade, vida privada, honra e imagem se aproximam dos dados pessoais por dizerem respeito a informações pessoais identificadas ou identificáveis, podendo conter dados sensíveis ou não. Ademais, até mesmo informações públicas abrangem os dados pessoais, estando cobertas pela nova normativa.

Mafei e Queiroz (2019, p. 19), partindo da construção teórica das normativas europeias,

entendem que a proteção de dados pessoais constitui um direito autônomo aos direitos fundamentais mencionados, sendo que o mero armazenamento em bancos de dados de informações de pessoas naturais, por si, faz emergir direitos subjetivos:

> Ao contrário do direito à privacidade, o direito à proteção de dados não faz, em princípio, um filtro substantivo sobre a qualidade do dado para decidir se ele está ou não em seu escopo: se é dado pessoal, interessa ao direito da proteção de dados pessoais, ainda que não seja sensível à privacidade do titular. Quando muito, poderá ter uma proteção incrementada (na qualidade de "dado pessoal sensível"), embora nem mesmo essa informação seja necessariamente sensível à privacidade do sujeito (como raça ou nacionalidade).
> Por isso, mesmo a informação pública (e dificilmente caracterizável com informação protegida pelo direito à privacidade) interessa ao direito à proteção de dados, se relacionar-se a indivíduo identificado ou identificável e for armazenada em banco de dados ou cadastros, sujeitos a tratamento automatizado ou não.

O reconhecimento da proteção dos dados pessoais como um direito autônomo e fundamental, para Doneda (2011), decorre da consideração da igualdade substancial, da liberdade e da dignidade da pessoa humana, bem como da proteção da intimidade e da vida privada. É também a partir da legislação infraconstitucional que esse direito se densifica, como demonstrado.

2.2 restrições à liberdade na pandemia: exceções democráticas ou estado de exceção?

Agamben (2020a, p. 23) explica que foi introduzido um novo conceito ao léxico político ocidental: o distanciamento social. Essa expressão que é colocada em momento de emergência sanitária global, segundo o autor italiano, questiona o que seria um ordenamento jurídico fundado sobre tal distanciamento. A mídia e as autoridades espalham um clima de pânico para provocar um verdadeiro Estado de Exceção como paradigma normal de governo. Nesse sentido, são aprovados decretos pelos governos por razões de higiene ou segurança, resultando em militarização de municípios (AGAMBEN, 2020a, p. 12).

Ao comentar a preocupação de Agamben, Boaventura de Sousa Santos (2020a, p. 14), afirma que essa inquietude – o Estado adquirir poderes excessivos a pretexto de tomar medidas de vigilância e restritivas de mobilidade no combate à pandemia, colocando em risco a democracia – não é fundada. Isso porque, para o autor português, as medidas restritivas não se tratam de um Estado de Exceção, mas de uma exceção em um Estado Democrático, que devem ser aceitas no cenário das aspirações e necessidades dos cidadãos comuns. Entretanto, Boaventura (2020) entende que a quarentena é discriminatória para os diversos grupos sociais. Esses grupos compõem o que o autor chama de sul, não enquanto um espaço geográfico, mas um espaço-tempo político, social e cultural, causado pela exploração capitalista, discriminação

racial e discriminação sexual. Ademais, Boaventura (2020) afirma que há grupos em relação aos quais a invasão da intimidade pode ser cada vez mais intrusiva, não obstante uma já pré-existente vulnerabilidade de diversos grupos sociais, o que torna a pandemia discriminatória. É possível verificar que cidadãos podem ficar ainda mais vulneráveis no período pandêmico.

É de se ressaltar, nesse cenário, a preocupação de Giorgio Agamben (2020b), que reconhece haver um novo momento de restrição de liberdades individuais, a pretexto de enfrentar urgências:

> Em muitas partes, vai se formulando agora a hipótese de que, na realidade, nós estamos vivendo o fim de um mundo, o das democracias burguesas, fundadas nos direitos, nos parlamentos e na divisão de poderes, que está dando lugar a um novo despotismo, que, no que diz respeito à perversidade dos controles e à cessação de toda atividade política, será pior do que os totalitarismos que conhecemos até agora. Os cientistas políticos estadunidenses o chamam de *"Security State"*, ou seja, um estado em que, "por razões de segurança" (neste caso de "saúde pública", termo que leva a pensar nos famigerados "comitês de saúde pública" durante o Terror), pode-se impor qualquer limite às liberdades individuais.
> Além disso, na Itália, estamos acostumados há muito tempo com uma legislação por decretos de urgência por parte do Poder Executivo, que, desse modo, substitui o Poder Legislativo e, de fato, abole o princípio da divisão dos poderes no qual se fundamenta a democracia. E o controle que é exercido por meio das câmeras de vídeo e agora, como foi proposto, por meio dos telefones celulares excede em muito toda forma de controle exercida sob regimes totalitários como o fascismo ou o nazismo.

Yara Frateschi (2020) explica o argumento de Agamben no sentido de que, ao se esgotarem as justificativas de restrição das liberdades individuais com base na alegação do terrorismo, é necessário encontrar um substituto, que no caso é o coronavírus. A autora assevera que, ao ser criado um estado de pânico coletivo, os indivíduos clamam por segurança e por restrição de liberdades, criando um "perverso círculo vicioso", em que os indivíduos trocam a liberdade por segurança, fomentando o Estado de Exceção.

A limitação de direitos fundamentais, antes de qualquer decisão sobre o tema, deve levar em consideração a excepcionalidade da medida em um contexto de pandemia de Covid-19, sem que haja a renúncia de liberdades individuais quando os critérios não são claros.

Não obstante, o discurso de renúncia ou restrição de liberdades individuais, sob pretexto de segurança, notadamente de dados pessoais (geodados), já foi observado em um importante julgamento pré-pandêmico.

Em 18 de setembro de 2019, o Tribunal Constitucional de Portugal debateu, por meio do Acórdão n. 464/2019 (PORTUGAL, 2019), a possibilidade de os serviços de telecomunicações terem acesso a metadados (nomes, números de telefone contatados, datas, tráfego de internet, entre outros). Questionou-se no referido julgado a constitucionalidade de duas normas que permitiam ao Estado Português o acesso a dados pessoais com o objetivo de

investigação de crimes, como terrorismo, sabotagem e outros, já tendo como norte a Diretiva 2016/679 do Parlamento Europeu e do Conselho. O fundamento dos 35 deputados que requereram a declaração de inconstitucionalidade foi a inviolabilidade de correspondência e das telecomunicações, permanecendo a possibilidade desse acesso em matéria processual criminal.

O Tribunal Português discutiu se seria possível que os dados pessoais (inclusive os seus geodados) de um indivíduo fossem compartilhados com os serviços de informação tão somente pela suspeita da prática de crime de terrorismo ou crime contra a segurança nacional, sem necessidade de pendência de um processo criminal. Os juízes entenderam que, em regra, o acesso de dados de telecomunicações e internet por oficiais de serviços de informação, tal como horário, duração e números envolvidos nas chamadas, violaria a Constituição Portuguesa. Todavia, os juízes entenderam que o acesso de dados pessoais como acesso à identificação e local de residência dos consumidores (utilizadores), o contrato de ligação à rede, bem como a posição geográfica, seria admitido para efeito de combate ao terrorismo. Justificaram a medida, de forma geral, para que fossem produzidas informações necessárias à prevenção de sabotagem, terrorismo etc., mas declararam inconstitucionais os motivos de salvaguarda nacional e segurança interna.

Esse julgado foi cercado pela polêmica (PÚBLICO, 2019a) da renúncia da juíza do Tribunal Constitucional Português, a ex-juíza Maria Clara Sottomayor, a qual afirmou ter sido selecionada por sorteio para ser relatora no "processo dos metadados". Na escolha do relator no tribunal, explica a ex-juíza, só participam os juízes que compõem a maioria previamente determinada, não sendo necessário alterar posteriormente o relator, portanto. A fundamentação do acórdão "será aquela que o relator construir e redigir, na sequência do debate e participação de todos os juízes, que propõem alterações ao texto e escrevem em declaração de voto as suas divergências". (PÚBLICO, 2019a). Entretanto, a ex-juíza do Tribunal Constitucional Português afirmou que o plenário assumiu um outro acórdão, mesmo que não tenha se negado a alterar o projeto do acórdão que apresentou. À vista do caráter vago que geraria a incerteza/indeterminação dos conceitos em análise, possibilitando que qualquer indivíduo pudesse ter seus dados devassados, a ministra Sottomayor entendeu pela inconstitucionalidade de todas as disposições indigitadas. O outro projeto de acórdão foi proferido pelo ministro Lino Rodrigues Ribeiro (PÚBLICO, 2019b), que veio a dar origem ao Acórdão n. 464/2019.

Com efeito, o acesso aos dados de base, consistente em informações sobre acesso à internet e moradia dos indivíduos, bem como os dados de localização, compostos pela posição geográfica, só seria possível nas hipóteses de combate ao terrorismo ou criminalidade organizada, devidamente autorizado. As justificativas de salvaguarda da defesa nacional e da

segurança interna não se mostraram plausíveis para o deferimento da medida, notadamente por serem conceitos indeterminados.

O julgado do Tribunal Constitucional Português é preocupante, posto que seria possível a devassa de dados pessoais, inclusive de geolocalização, sem a necessidade de um processo criminal em curso, autorizando-se o compartilhamento ao Estado de informações a partir de meras suspeitas de cometimento de crimes graves. Ademais, o Tribunal Português concordou em retirar garantias do cidadão para os fins de prevenção de sabotagem, terrorismo e outros, inclusive os dados pessoais de geolocalização, o que já indicava a tendência de flexibilização das garantias constitucionais antes da pandemia. É importante notar que no "processo dos metadados" do Supremo Tribunal de Justiça Português o julgamento esteve circunscrito à necessidade de restrição da liberdade, ou seja, da disponibilização de dados pessoais em razão da prevenção criminal, o que causa possível aplicação, com relativização de direitos fundamentais na pandemia de Covid-19.

Os tempos de pandemia exigem cautela, ou seja, não se pode tomar medidas extremadas, que possam atingir direitos e garantias fundamentais. Utilizar uma situação de calamidade pública para vilipendiar e punir quem exerce direitos constitucionalmente consagrados equivaleria a abrir uma porta à arbitrariedade, criando um precedente perigoso em termos de direitos fundamentais. Daí que emerge a pertinência do posicionamento de Agamben, posto que a pandemia de Covid-19 se inseriria em um contexto de aceleração da restrição da privacidade e da intimidade dos cidadãos, mediante uma menor proteção dos dados pessoais, inclusive os geodados.

Emerge também a relevância do marco teórico de Robert Alexy (2015) para o qual não existem direitos fundamentais absolutos, sejam coletivos ou individuais, haja vista a necessidade de convivência deles no ordenamento. Ao discutir a relação entre o direito e a sua restrição, o autor sugere que se tratariam de duas categorias distintas – o direito e a restrição –, identificando-a como *teoria externa* (ALEXY, 2015, p. 277). Não haveria uma relação necessária entre essas duas categorias, que se estabeleceria "pela necessidade de compatibilização concreta entre os diversos tipos de direitos fundamentais" (MENDES; BRANCO, 2015, p. 198).

Contrapõe-se a essa ideia a *teoria interna*, em que o "conceito de restrição é substituído pelo conceito de limite" (ALEXY, 2015, p. 277) e sustenta-se na concepção de que "o direito com um determinado conteúdo" (ALEXY, 2015, p. 277). Nesse caso, "eventual dúvida sobre o limite do direito não se confunde com a dúvida sobre a amplitude das restrições que lhe devem ser impostas, mas diz respeito ao próprio conteúdo do direito" (MENDES; BRANCO, 2015, p.

198), de forma que a parte restringida não se trataria de um direito fundamental.

No caso dos princípios fundamentais da privacidade e da intimidade, que se contrapõem neste caso em concreto com a segurança em período de calamidade de Covid-19, percebe-se que a *teoria interna* dificilmente poderia desatar o problema, na medida em que considera os direitos fundamentais como regras, não susceptíveis de restrições; ao passo que a *teoria externa* admitira as restrições a princípios, guiada pelo sopesamento.

Verifica-se, portanto, que há a necessidade de que o ente que possuir os dados de geolocalização do cidadão garanta instrumentos para mitigar ou eliminar riscos de disseminação indiscriminada de dados. Este ente, seja o Estado, uma empresa concessionária do serviço público ou uma empresa não concessionária (*Google*, aplicativos móveis e outros) deve assumir uma postura ética frente à nova normativa de proteção de dados.

2.3 Os aplicativos móveis para alerta e prevenção da covid-19

Na Coreia do Sul, são vários os *sites* e aplicativos de *smartfones* que surgiram para coletar e mapear dados que, em auxílio aos testes e ao isolamento, ajudaram a reduzir a disseminação do vírus. Muito embora as informações sejam úteis para os epidemiologistas, há entendimento de que se corre o risco do estigma caso sejam divulgadas à sociedade, observado que a preocupação com a privacidade e a transparência dos processos na Coreia do Sul remonta desde o surto de coronavírus de 2015, que foi denominado MERS (*Nature*, 2020).

Dentre as preocupações com os aplicativos em *smartphones* está a "normalização" de estruturas de vigilância, como explica Diego Aranha, professor do departamento de Engenharia da Aarhus University, na Dinamarca (BBC, SCHREIBER, 2020):

> A estrutura de vigilância, depois de montada, é muito difícil de ser revertida. Por mais que seja justificada a necessidade de se instalar agora, para esse caso específico, é muito tentador para governos rapidamente encontrarem outras formas de usar aquela mesma infraestrutura de vigilância, que fica normalizada e pode se tornar permanente.

Argumenta-se, por outro lado, que o risco na utilização de dados anônimos e agregados é baixo e pouco invasivo (BBC, SCHREIBER, 2020).

A geolocalização dos indivíduos e posterior fornecimento ao Estado também está sendo realizada pelo *Google* (CANALTECH, 2020):

> O Google está usando dados de geolocalização dos usuários para elaborar relatórios direcionados às organizações e autoridades de saúde, a fim de auxiliar as entidades a medir o volume do isolamento social causado pelo avanço do vírus SARS-CoV-2 pelo mundo e determinar se as pessoas estão de fato seguindo as recomendações de quarentena estipuladas pela Organização Mundial da Saúde (OMS).

O *Google* está sofrendo críticas em razão de compartilhamento de dados de

geolocalização dos usuários sem o consentimento dos usuários. Isso porque a empresa exige que a localização dos aparelhos celulares esteja ligada para que que aplicativos de *contact tracing* da Covid-19 possam funcionar, que recorrem apenas à função de *bluetooth* desses aparelhos. Segundo noticiou o *The New York Times*, a tecnologia está sendo alvo de críticas, visto que, em tese;

> [...] ao exigir que os utilizadores tenham o acesso à localização ligado, a Google é capaz de obter a localização de um determinado utilizador com alta precisão. Tal nunca foi a intenção do contact tracing à Covid-19 através da utilização exclusiva de códigos aleatórios gerados e emitidos por Bluetooth, como tem sido reiteradamente apontado pelo INESC TEC, numa altura em que a Comissão Europeia também já criticou o uso de georreferenciação para este efeito (ECO, 2020).

Alexandra Aragão (2020) entende que os dados produzidos pelos aplicativos móveis para alerta e prevenção da Covid-19 parecem ser uma resposta que pode auxiliar as autoridades na contenção da propagação do vírus. Isso porque esses dados, anonimizados e agregados, podem auxiliar na compreensão da propagação do vírus, na avaliação da eficácia das medidas de distanciamento social, na modalização da dinâmica espacial das epidemias e dos efeitos econômicos da crise. A autora acrescenta que as tecnologias digitais vão mudar a vida cotidiana, tais como a automação, a internet das coisas, os sistemas baseados em inteligência artificial, tecnologia 5G e as aprendizagens de máquina e profunda, sendo que a conectividade propiciada pelo uso de novas tecnologias tem o potencial de melhorar a saúde e o bem-estar, as finanças pessoais, a sustentabilidade ambiental, entre outros benefícios (ARAGÃO, 2020).

Não se discute a aceitação das tecnologias para alcançar importantes objetivos sociais e ambientais, mas as condições de segurança da informação para o cidadão. Em consequência da maior geração e processamento de dados em dispositivos de comunicação e serviços digitais, há o aumento dos riscos de discriminação, práticas desleais e efeitos de dependência. Além disso, há o risco da facilitação da criminalidade clássica (crimes patrimoniais e contra a vida), da *cibercriminalidade* (devassa de telecomunicações) e do risco de vigilância massiva da população ou que a mesma se dê de forma discriminatória (ARAGÃO, 2020).

Para que os dispositivos móveis de alerta e detecção de Covid-19 não tensionem abusivamente os direitos fundamentais, Aragão (2020) aduz que os aplicativos devem buscar garantir mecanismos para conferir a intimidade e a privacidade dos utilizadores por meio da *cibersegurança*, para que seja diminuído o risco de discriminação, assim como assegurar o bem-estar social e ambiental. Dentre os mecanismos que a autora descreve terem sido fundamentais para a preservação de direitos fundamentais, são cinco as condições capazes de reforçar a confiança e viabilizarem a utilização das tecnologias digitais de geolocalização na pandemia: (a) os aplicativos de geolocalização podem surgir do Estado ou da iniciativa privada,

mas devem depender de aprovação do primeiro, respeitando requisitos regulamentares e éticos; (b) a adesão deve ser facultativa, podendo o utilizador dar o consentimento e acionar o envio dos dados, assim como o sistema não poderá ser dependente de uma única adesão, de tudo ou nada, mas cada envio poderá ser deliberado; (c) os aplicativos de geolocalização devem servir apenas para vigilância epidemiológica da Covid-19 ou para doenças similares, e os dados somente podem ser acessados por autoridades de saúde; e (d) os aplicativos de geolocalização somente funcionarão enquanto perdurar a epidemia, deixando os mesmos de funcionar sozinhos (ARAGÃO, 2020).

No tocante às novas tecnologias de rastreamento de contato digital, Kahn *et al* (2020, p. 18/19) advertem que deve haver uma abordagem gradual que priorize o alinhamento da tecnologia com as necessidades de saúde pública e os valores públicos, criando opções na arquitetura de design e capturando resultados e impactos do mundo real para permitir ajustes conforme necessário. Além disso, diante de questões intrincadas a serem resolvidas por governos e pelas empresas, recomenda-se o envolvimento público e avaliações contínuas para melhorar o desempenho dessas novas tecnologias (KAHN et al, 2020, p. 19).

Os princípios que devem orientar o uso das novas tecnologias de saúde pública de rastreamento de contato digital para resposta à pandemia são (a) o envolvimento dos líderes governamentais, de saúde e de tecnologia digital, de forma eficaz com o público para comunicar sobre a utilidade, a importância e limitações das tecnologias digitais que são utilizadas, incluindo suas implicações para a privacidade e as liberdades dos indivíduos; (b) a transparência em todos os níveis é essencial para manter a confiança do público; (c) o reconhecimento por parte dos tomadores de decisão, dos sacrifícios que algumas pessoas podem estar dispostas a fazer durante uma pandemia para promover as metas de saúde pública, ou seja, a aceitação de alguns recursos de monitoramento específicos não deve ser interpretada como uma disposição de estender esses métodos a outros problemas ou usos; (d) se estratégias escolhidas de saúde pública digital violarem a privacidade e outras liberdades civis, as violações devem ser suficientemente justificadas pelas circunstâncias da pandemia, compensadas pelo amplo benefício público previsto, e consideradas relativas às violações associadas a outras estratégias possíveis, tais como distanciamento físico; (e) apenas os dados necessários e relevantes para os objetivos de saúde pública declarados devem ser coletados, sendo que os dados identificáveis devem ser armazenados de forma segura e apenas pelo período de tempo que os objetivos de saúde pública exigirem; (f) as tecnologias adotadas não devem ser usadas de maneiras que sujeitem as comunidades à discriminação ou vigilância por razões não públicas de saúde; (g) o respeito pela autonomia individual requer que os usuários estejam suficientemente informados

sobre os objetivos de saúde pública da tecnologia e até que ponto esses objetivos estão sendo alcançados; (h) a responsabilidade e consequências do abuso e uso indevido dos dados devem ser claros e aplicáveis; (i) as tecnologias digitais de saúde pública devem ser implantadas de uma maneira que não propague padrões preexistentes de desvantagem injusta ou distribua ainda mais danos e riscos injustamente pela população; (j) na medida do possível, as tecnologias digitais de saúde pública devem ser projetadas para corrigir as desigualdades existentes; (k) os incentivos e desincentivos para a adoção de novas tecnologias devem ser equitativos, não exploradores e alinhados com o uso eficaz da tecnologia; (l) as lacunas de tecnologia motivadas pela disparidade devem ser explicitamente reconhecidas, logo, na medida do possível, devem ser tomadas providências para lidar com a exclusão digital (KAHN et al, 2020, p. 23/24).

Assim, a discussão em torno das novas tecnologias digitais de rastreamento de contato merece atenção no que se refere aos direitos à intimidade e à privacidade, os quais são inevitavelmente atingidos, notadamente quando estudados os dados que indicam a localização dos indivíduos, os chamados geodados. Não obstante, em tempo de pandemia da Covid-19, o debate agrega um novo componente, a utilização dos geodados para rastreamento, que poderia trazer restrições ainda maiores à intimidade e à privacidade.

2.4 O vazamento de (geo)dados e a defesa em juízo a intimidade e da privacidade e os dados pessoais (de geolocalização) como direito coletivo

Ante diversas notícias que dão conta do vazamento de dados pessoais, percebe-se que o risco à intimidade e à privacidade é real e urgente, principalmente em relação aos geodados e outros dados sensíveis. Considerados o aumento exponencial dos dados e dos valores atrelados a eles, são potencializados também os vazamentos. O vazamento de dados é fato que ocorre com uma frequência que preocupa, à vista das notícias que grassam cotidianamente. Machado *et al* (2019) informam que "notícias e relatório de segurança sobre vazamentos de dados sensíveis têm surgido com uma frequência cada vez maior" sendo "muitos desses vazamentos, cujo volume e criticidade são altos, vêm afetando empresas e governos de forma significativa".

Nesse contexto, a LGPD previu medidas preventivas para eventuais vazamentos do operador, que é a pessoa que realizará o tratamento dos dados pessoais, dando respostas a essa violação de direitos. Dentre elas está a anonimização dos dados pessoais, consistente na utilização de meios técnicos para não ser possível a associação, direta ou direta, a um indivíduo, que é necessária quando os referidos dados forem franqueados a órgão de pesquisa. É visível

que a utilização dos dados pela sociedade e pelo Estado ultrapassa o interesse consumerista, principalmente o compartilhamento de dados (uso compartilhado de dados, nos termos da LGPD) a partir da pandemia da Covid-19, emergindo discussões acerca da privacidade dos indivíduos.

Nesse particular, a Medida Provisória n. 954/2020 (BRASIL, 2020c) permitiu, durante a sua vigência, o compartilhamento de dados por empresas de telecomunicações prestadoras de Serviço Telefônico Fixo Comutado e de Serviço Móvel Pessoal com a Fundação Instituto Brasileiro de Geografia e Estatística (IBGE), para fins de propiciar suporte à produção estatística oficial durante a situação de emergência de saúde pública de importância internacional decorrente do coronavírus (Covid-19), de que trata a Lei n. 13.979, de 6 de fevereiro de 2020. O referido uso compartilhado de dados de geolocalização de indivíduos em todo o País por empresas de telecomunicações e de tecnologia com o IBGE teria o objetivo primário de viabilizar a produção de estatísticas. A Medida Provisória teve seu prazo encerrado quatro meses após sua edição, sem conversão em lei. É necessário observar que as medidas de compartilhamento de dados pessoais de geolocalização promovidas pela MP 954/2020 (BRASIL, 2020c) foram fundamentada na urgência pública de saúde do monitoramento da pandemia de Covid-19 em território nacional. A exposição de motivos da referida normativa afirmava que "[...] o IBGE necessita ter acesso a informações sobre o número de telefone e respectivo endereço residencial dos consumidores de serviços de telecomunicações, de pessoas naturais ou jurídicas" (BRASIL, 2020d). Ao contrário do informado em sua exposição de motivos, a Medida Provisória não se limitava a dispor sobre o compartilhamento de número de telefone e endereço residencial de consumidores, mas inclusive previu a disponibilização de seus nomes. Nesse contexto hostil à privacidade e à intimidade, a MP 954/2020 (BRASIL, 2020c) permitiu a disponibilização de dados pessoais, como relação dos nomes, dos números de telefone e dos endereços de seus consumidores, pessoas físicas ou jurídicas, sem que se orientasse por uma completa salvaguarda de dados, possibilitando a identificação direta ou indireta, ou seja, sem garantir a privacidade do indivíduo.

Além disso, a grande limitação aos direitos à privacidade e à intimidade decorrente da MP 954/2020 (BRASIL, 2020c) e dos consequentes compartilhamentos de dados entre empresas de telecomunicações e o Estado encontra outro obstáculo, qual seja, não ter ocorrido por intermédio de lei em sentido estrito. A referida MP foi bastante contestada pela sociedade enquanto esteve vigente, à vista das cinco ações diretas de inconstitucionalidade propostas. Dentre elas, houve pedido de medida cautelar na ADI 6.388, relatada pela ministra Rosa Weber, contra o inteiro teor da MP, na qual foram aduzidos vícios formais de inconstitucionalidade, por

ausência dos requisitos para edição de medida provisória, assim como inconstitucionalidade material, em razão de violação das regras constitucionais da dignidade humana, inviolabilidade da intimidade, vida privada, honra e imagem das pessoas, sigilo dos dados e autodeterminação informativa. Embora não tenha subestimado a gravidade e a urgência no compartilhamento de dados pessoais decorrentes da crise atual, em sua fundamentação, a ministra argumenta que os direitos à privacidade e à autodeterminação informativa foram positivados na LGPD. Considerou-se que a MP n. 954/2020 constituía invasão injustificada na privacidade individual do indivíduo, por compreender que a MP "não apresenta mecanismo técnico ou administrativo apto a proteger os dados pessoais de acessos não autorizados, vazamentos acidentais ou utilização indevida".

As medidas provisórias são atos do poder executivo a serem utilizadas em situações excepcionais, todavia, não raras vezes são desvirtuadas. São exigidos os requisitos do art. 62 da Constituição, quais sejam, relevância e urgência. No caso tratado, ainda que se possa interpretar desta forma em razão da emergência de saúde pública que vive o País, o fato é que não há, como há no caso da Lei n. 9.296/1996 (BRASIL, 1996), mecanismos de controle ou qualquer garantia assegurada às pessoas ou à coletividade por conta de eventuais desvios e abusos praticados. Vale dizer, foi autorizada uma violação de direitos, mediante interpretação subjetiva da norma constitucional, de eficácia duvidosa e sem o necessário controle e limite.

É importante notar que não há, por si, uma negativa do compartilhamento de dados, mas a necessidade de uma melhor estruturação técnica e jurídica para que ocorra esse compartilhamento, mesmo em tempos excepcionais de pandemia. Apesar do reconhecido interesse público no compartilhamento de dados pessoais, seria imperioso adotar salvaguardas para proteção dos mesmos.

A MP teve seu prazo de vigência encerrado e não foi convertida em lei.

O Tribunal de Justiça do Estado de São Paulo também está engajado na controvérsia do compartilhamento de dados pessoais de geolocalização. Por meio do mandado de segurança n. 2.069.736-76.2020.8.26.0000, o impetrante (um cidadão) fundamentou existir grave e iminente ameaça de privacidade e do direito de ir e vir, porquanto foi celebrado um acordo de cooperação entre o governo do Estado e as empresas de telefonia para compartilhamento de geodados para monitoramento e controle da pandemia. Foi sustentado que tal medida somente seria possível em estado de sítio ou para fins de monitoramento de condenado criminal ("tornozeleira eletrônica"), havendo infringência da legislação internacional, constitucional e infraconstitucional. No acórdão, o magistrado entendeu inexistir violação do direito do impetrante, haja vista ter assegurado o não tratamento de dados pessoais pelo Estado, pois

seriam todos anonimizados, agregados, estatísticos e volumétricos, não podendo ser identificado o seu titular. Ademais, foi ressaltada a necessidade de adoção de medidas restritivas de isolamento social pelo Estado, visando ao enfrentamento da pandemia, resguardando direitos fundamentais da vida e da saúde. Inclusive, seriam apuradas tão somente regiões com maior movimentação de pessoas. Em outras palavras, "assegurado o anonimato, preservado o sigilo dos dados apurados pelas empresas de telefonia móvel antes da transferência ao IPT, não há afronta a direito individual" (SÃO PAULO, 2020).

Necessário destacar nesse cenário a utilização de princípios específicos do processo coletivo, como o da máxima defesa dos direitos e interesses difusos e coletivos, além da efetivação da segurança jurídica. O fornecimento de dados de geolocalização era em sua maioria trabalhado no campo penal, mas no contexto da pandemia ultrapassa as fronteiras criminais e deságua na sociedade a título de direito difuso. Importante mencionar a indivisibilidade do objeto, em que a ofensa, de fato ao direito de um, constitui ofensa, ao menos em tese, ao direito de todos.

Registre-se que o artigo 1º da LGPD, já em completa vigência, possui a seguinte redação:

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

Mais do que um direito fundamental individual, pode-se perceber pelo teor da lei que se trata de um direito coletivo e de interesse nacional (art. 2º), o qual atinge um número indeterminado de pessoas. Umas das razões intrínsecas que se levanta para a necessidade da existência da lei em questão ultrapassa um direito fundamental individual e repousa na manutenção e evolução do próprio Estado Brasileiro.

A própria Constituição estabelece em seu art. 3º que os objetivos fundamentais da República Federativa do Brasil, dentre os quais se destaca a garantia do desenvolvimento nacional. Para que este objetivo seja levado a efeito, há que se trabalhar em conjunto, dentre outros fatores, com a dinâmica da ordem econômica e financeira, cujos princípios estão elencados no artigo 170 da Constituição da República.

Nessa perspectiva e levando em consideração a relação apresentada, a observância da LGPD pode contribuir para o desenvolvimento do pensamento jurídico nacional, concretizando e solidificando os direitos consagrados no ordenamento jurídico brasileiro.

Salvo situações excepcionais, a proteção de uma pessoa equivale à proteção de todos, daí porque se pode dizer que o objeto é indivisível. Da mesma forma o maltrato ou a falha em

relação a uma única pessoa tem o condão de comprometer a segurança que a todos deve ser destinada. Por esta razão, pode-se afirmar que se está diante de um interesse difuso. Nesse prisma, insere-se a defesa do objeto previsto na lei, no microssistema processual coletivo formado mormente por meio da Lei da Ação Civil Pública (BRASIL, 1985), da Lei da Ação Popular (BRASIL, 1965) e do Código de Defesa do Consumidor (BRASIL, 1990), sendo passível de tutela por meio do processo coletivo.

Conquanto o rastreamento de dados pessoais de localização possa oportunizar arbitrariedades, seja por práticas do Estado ou por empresas, é possível estabelecer limites éticos, técnicos e jurídicos (processuais e materiais) para proteção individual, mesmo em período de pandêmico, quando se exigem medidas acentuadas.

Espelhada em documentos internacionais, especialmente da União Europeia, a LGPD tem o potencial de cumprir com os seus objetivos, ainda que o compartilhamento de dados por geolocalização deva ser aprimorado nos âmbitos normativo e regulamentar, principalmente à vista do prazo de vigência encerrado da MP n. 954/2020.

3 CONCLUSÃO

Uma das grandes diferenças entre os chamados países desenvolvidos e os que não atingiram esse patamar é a forma com que atravessam e geram suas crises. Enquanto nos primeiros o respeito à regra serve de amparo e impulso à evolução e superação, nos outros, as regras constituem entraves para medidas de emergência, sem transparência e de flexibilização de direitos, isso tudo com a chancela da maioria das instituições públicas. Nessa seara, alguns países em desenvolvimento, como o Brasil, a sociedade se torna um laboratório de experiências legislativas altamente problemático.

Os dados são um bem de inequívoco valor para a sociedade e para o Estado, os quais devem ser utilizados de forma responsável e sustentável, observando-se principalmente os direitos fundamentais da intimidade e da privacidade.

Nesse sentido, a geração exponencial de dados, o surgimento das tecnologias digitais e a conectividade que é oportunizada podem trazer ganhos sociais e ambientais à sociedade e ao Estado, mas deve haver cautela no estabelecimento de diretrizes para o uso e compartilhamento de dados pessoais, sejam sensíveis ou não, de forma a criar mecanismos de proteção dos mesmos.

Os dados pessoais de geolocalização ou geodados, por exemplo, claramente possuem valor no estabelecimento de políticas públicas para o enfrentamento da pandemia do Covid-19,

mas exige o estabelecimento de normas claras e específicas para prever e evitar a vulneração massiva de direitos fundamentais dos cidadãos.

A discussão ultrapassa a própria pandemia de Covid-19, na medida em que já eram lançadas antes desta calamidade pública medidas restritivas de liberdades individuais sob o fundamento de segurança.

Não se trata, portanto, tão somente do risco de vazamento de dados pessoais, mas também da criação de mecanismos além daqueles previstos pela LGPD, mitigando e eliminando riscos no recebimento e no tratamento dos dados pessoais pelo operador, seja no âmbito do Estado ou da sociedade.

4 REFERÊNCIAS

AGAMBEN, G. **Reflexões sobre a peste.** Trad. Isabella Marcatti. São Paulo: Boitempo, 2020a.

AGAMBEN, G. Pandemia, novas reflexões. Entrevista com Giorgio Agamben. **Revista IHU On-line,** 23 abr. 2020. 2020b. Disponível em: http://www.ihu.unisinos.br/78-noticias/598295-pandemia-novas-reflexoes-entrevista-com-giorgio-agamben. Acesso em: 08 set. 2022.

ALEXY, R. **Teoria dos direitos fundamentais.** Trad. Virgílio Afonso da Silva. 2. ed. São Paulo: Ed. Malheiros, 2015.

ARAGÃO, A. **Questões ético-jurídicas relativas ao uso de apps geradoras de dados de mobilidade para vigilância epidemiológica da Covid-19**: uma perspectiva Europeia. Disponível em: https://www.uc.pt/covid19/documentos/artigoalexandraaragao Acesso em: 08 set. 2022.

BBC. SCHREIBER, M. Coronavírus: uso de dados de geolocalização contra a pandemia põe em risco sua privacidade? Disponível em https://www.bbc.com/portuguese/brasil-52357879 Acesso em: 08 set. 2022.

BRASIL. Constituição da República Federativa do Brasil de 1988. Brasília, 5 de outubro de 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 08 set. 2022.

BRASIL. Lei n. 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. Brasília. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078.htm Acesso em: 08 set. 2022.

BRASIL. Emenda Constitucional n. 17, de 03 de julho de 2019. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Senado Federal, Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2210757. Acesso em: 08 set. 2022.

BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm Acesso em: 08 set. 2022.

BRASIL. Lei n. 12.965, de 23 de abril de 2014. "Marco Civil da Internet". Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 08 set. 2022.

BRASIL. Lei Complementar n. 105, de 10 de janeiro de 2001. Dispõe sobre o sigilo das operações de instituições financeiras e dá outras providências. Brasília. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/lcp/lcp105.htm. Acesso em: 08 set. 2022.

BRASIL. Lei n. 9.296, de 24 de julho de 1996. "Lei de Interceptação Telefônica". Regulamenta o inciso XII, parte final, do art. 5° da Constituição Federal. Disponível em: http://www.planalto.gov.br/ccivil_03/LEIS/L9296.htm Acesso em: 08 set. 2022.

BRASIL. Medida Provisória n. 959, de 29 de abril de 2020. 2020a. Estabelece a operacionalização do pagamento do Benefício Emergencial de Preservação do Emprego e da Renda e do benefício emergencial mensal de que trata a Medida Provisória nº 936, de 1º de abril de 2020, e prorroga a vacatio legis da Lei nº 13.709, de 14 de agosto de 2018, que estabelece a Lei Geral de Proteção de Dados Pessoais - LGPD. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2020/Mpv/mpv959.htm Acesso em: 08 set. 2022.

BRASIL. Exposição de Motivos n. 168/2020. Medida Provisória 959/2020. 2020b. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2020/Exm/Exm-MP-959-20.pdf Acesso em: 08 set. 2022.

BRASIL. Medida Provisória n. 954, de 17 de abril de 2020. 2020c. Dispõe sobre o compartilhamento de dados por empresas de telecomunicações prestadoras de Serviço Telefônico Fixo Comutado e de Serviço Móvel Pessoal com a Fundação Instituto Brasileiro de Geografia e Estatística, para fins de suporte à produção estatística oficial durante a situação de emergência de saúde pública de importância internacional decorrente do coronavírus (covid-19), de que trata a Lei nº 13.979, de 6 de fevereiro de 2020. Disponível em: http://www.planalto.gov.br/CCIVIL_03/_Ato2019-2022/2020/Mpv/mpv954.htm Acesso em: 08 set. 2022.

BRASIL. Exposição de Motivos n. 151/2020. Medida Provisória 954/2020. 2020d. Disponível em: http://www.planalto.gov.br/CCIVIL_03/_Ato2019-2022/2020/Mpv/mpv954.htm Acesso em: 08 set. 2022.

BRASIL. Superior Tribunal de Justiça. REsp 1726270/BA, Rel. Ministra NANCY ANDRIGHI, Rel. p/ Acórdão Ministro RICARDO VILLAS BÔAS CUEVA, TERCEIRA TURMA, julgado em 27/11/2018, DJe 07/02/2019.

CANALTECH. **Google usa geolocalização de usuários para medir isolamento social pela COVID-19**. Disponível em https://canaltech.com.br/internet/google-usa-geolocalizacao-de-usuarios-para-medir-isolamento-social-pela-covid-19-162851/ Acesso em: 08 set. 2022.

CATE, F. H.; CULLEN, Peter; MAYER-SCHÖNBERGER, Viktor. **Data protection principles for the 21st century**: revising the 1980 OECD guidelines. Redmond, WA: Microsoft Corporation (2014). Disponível em: https://www.oii.ox.ac.uk/archive/downloads/publications/Data_Protection_Principles_for_the_21st_Century.pdf. Acesso em: 08 set. 2022.

DONEDA, D. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico Journal of Law**, 2011, v. 12, n. 2, p. 91-108. Disponível em: https://portalperiodicos.unoesc.edu.br/espacojuridico/article/view/1315. Acesso em: 08 set. 2022.

ECO. **Portugal pressiona Google a desligar acesso ao GPS na app de "contact tracing"**. Disponível em https://eco.sapo.pt/2020/07/21/portugal-pressiona-google-a-desligar-acesso-ao-gps-na-app-de-contact-tracing/ Acesso em: 08 set. 2022.

FRATESCHI, Y. **Agamben sendo Agamben**: o filósofo e a invenção da pandemia. Disponível em: https://blogdaboitempo.com.br/2020/05/12/agamben-sendo-agamben-o-filosofo-e-a-invencao-da-pandemia/ Acesso em: 08 set. 2022.

JULIO, R. A. "Dados são o novo petróleo", diz CEO da Mastercard – exceto por um pequeno detalhe: para ajay banga, internet das coisas é a mais impactante tecnologia da transformação digital. **Época Negócios.** 05 jul. 2019. Disponível em: https://epocanegocios.globo.com/Empresa/noticia/2019/07/dados-sao-o-novo-petroleo-diz-ceo-da-mastercard.html Acesso em: 08 set. 2022.

KAHN, Je. P. et al. (ed.). **Digital contact tracing for pandemic response**: Ethics and governance guidance. Johns Hopkins University Press, 2020.

MACHADO, R.; KREUTZ, D.; PAZ, G.; RODRIGUES, G. Vazamentos de Dados: Histórico, Impacto Socioeconômico e as Novas Leis de Proteção de Dados. In: 4° **Workshop Regional de Segurança da Informação e de Sistemas Computacionais**. Disponível em: https://sol.sbc.org.br/index.php/errc/article/view/9230. Acesso em: 08 set. 2022.

MENDES, G. F.; BRANCO, G. G. **Curso de direito constitucional.** 10 ed. São Paulo: Saraiva, 2015.

NATURE. **South Korea is reporting intimate details of COVID-19 cases: has it helped?** Extensive contact tracing has slowed viral spread, but some say publicizing people's movements raises privacy concerns. Disponível em https://www.nature.com/articles/d41586-020-00740-y Acesso em: 08 set. 2022.

QUEIROZ, R. M. R. Direito à privacidade e proteção de dados pessoais: aproximações e distinções. In: **Revista do Advogado**. Ano XXXIX. N. 144. Nov. 2019.

OCDE. **OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data**. Disponível em: http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm. Acesso em: 08 set. 2022.

PORTUGAL. Tribunal Constitucional. Acórdão nº 464 (Processo n.º 26/2018). Plenário.

Julgado em 18 de setembro de 2019. Disponível em https://www.tribunalconstitucional.pt/tc/acordaos/20190464.html. Acesso em: 08 set. 2022.

PÚBLICO. Quem guarda o guardador? 2019a. Disponível em https://www.publico.pt/2019/09/23/politica/opiniao/guarda-guardador-1887519. Acesso em: 08 set. 2022.

PÚBLICO. "É a minha honra de juíza". 2019b. Disponível em https://www.publico.pt/2019/12/09/politica/opiniao/honra-juiza-1896464. Acesso em: 08 set. 2022.

SÃO PAULO. Tribunal de Justiça. Órgão Especial. Ms Nº 2.069.736-76.2020.8.26.0000. Voto nº 43.067. Impte. CAIO JUNQUEIRA ZACHARIAS. Impdo. GOVERNADOR DO ESTADO DE SÃO PAULO. Relator: Desembargador Evaristo dos Santos. São Paulo, SP, 24 de junho de 2020. Dje. São Paulo, 25 jun. 2020.

SOUSA SANTOS, B. **A cruel pedagogia do vírus**. São Paulo: Boitempo, 2020.

TATEOKI, V. A. **O uso dos dados pessoais como mecanismo de persuasão no processo de tomada de decisão dos usuários de internet.** 2019. 198 f. Dissertação (Mestrado) - Curso de Direito, Fmu, São Paulo, 2019. Disponível em: https://arquivo.fmu.br/prodisc/mestradodir/vat.pdf. Acesso em: 08 set. 2022.

UNIÃO EUROPEIA. Regulamento 2016/679 do Parlamento Europeu e do Conselho. Regulamento Geral sobre a Proteção de Dados, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679. Acesso em: 08 set. 2022.

UNIÃO EUROPEIA. Convenção para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal. Conselho da Europa. Disponível em: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108. Acesso em: 08 set. 2022.

UNIÃO EUROPEIA. Diretiva 95/46. CE do Parlamento Europeu e do Conselho de 24 de outubro de 1995 relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre-circulação desses dados, 1995. Disponível em: https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=CELEX%3A31995L0046. Acesso em: 08 set. 2022.