Centro Universitário de Brasília - CEUB

Faculdade de Ciências Jurídicas e Sociais - FAJS
Curso de Bacharelado em Direito

ISABELA MARTINS DA CUNHA

OS SISTEMAS DE MONITORAMENTO E O PODER DOS ALGORITMOS: análise a partir do contexto da pandemia do coronavírus

BRASÍLIA
2022

ISABELA MARTINS DA CUNHA

OS SISTEMAS DE MONITORAMENTO E O PODER DOS ALGORITMOS: análise a partir do contexto da pandemia do coronavírus

Artigo científico apresentado como requisito parcial para obtenção do título de Bacharel em Direito pela Faculdade de Ciências Jurídicas e Sociais - FAJS do Centro Universitário de Brasília (UniCEUB).

Orientador: Professor Humberto Cunha dos Santos

BRASÍLIA
2022

ISABELA MARTINS DA CUNHA

OS SISTEMAS DE MONITORAMENTO E O PODER DOS ALGORITMOS: análise a partir do contexto da pandemia do coronavírus

Artigo científico apresentado como requisito parcial para obtenção do título de Bacharel em Direito pela Faculdade de Ciências Jurídicas e Sociais - FAJS do Centro Universitário de Brasília (UniCEUB).

Orientador: Professor Humberto Cunha dos Santos

BRASÍLIA, 2022

BANCA AVALIADORA

_____

Professor Humberto Cunha dos Santos

_____

Professor(a) Avaliador(a)

OS SISTEMAS DE MONITORAMENTO E O PODER DOS ALGORITMOS: análise a partir do contexto da pandemia do coronavírus

Isabela Martins da Cunha

RESUMO

O presente artigo científico se dedicou a delinear os possíveis riscos à privacidade e à proteção de dados pessoais em contextos de crises epidemiológicas, como o caso da pandemia do coronavírus. A despeito de todas as partes do mundo terem sido acometidas com o vírus e terem, consequentemente, sofrido eventual violação ao direito à proteção de dados pessoais, o artigo procurou destacar como, no Brasil, há circunstâncias peculiares que revelam um estágio incipiente de adequação à legislação nacional de proteção de dados, não havendo no país uma "cultura de proteção de dados". Assim, em meio a um cenário de implementação de sistemas de monitoramento para que fosse possível controlar a disseminação da COVID-19, o texto procurou retratar como o direito à proteção de dados pessoais estava desemparado, gerando má utilização em diversos aspectos referentes à coleta e tratamento de dados pessoais. Para discutir tal temática, foram analisados os casos das tecnologias implantadas em São Paulo e em Recife, os quais coletaram dados de geolocalização para aferir a adesão ao isolamento social. Ao final, foram apresentadas conclusões que, a partir da experimentação vivenciada na coleta e tratamento de dados pessoais durante a pandemia, realçam a importância de ações públicas e privadas que priorizem a privacidade e a proteção de dados pessoais para permitir a adequada proteção desses direitos.

Palavras-chave: Privacidade. Proteção de Dados Pessoais. COVID-19. Sistemas de monitoramento. Dados de geolocalização. *Profiling*. Dados anonimizados. Danos agregados. Privacidade de grupo. Discriminação algorítmica.

SUMÁRIO

INTRODUÇÃO

Com o início da pandemia da COVID-19, a sociedade viu-se, mais do que nunca, imersa e dependente do ambiente digital e dos recursos tecnológicos. Com o intuito de controlar a disseminação do coronavírus, os governos realizaram parcerias com operadoras de telefonia e com empresas especializadas em tecnologia e implementaram sistemas de monitoramento, que coletam dados de geolocalização de forma agregada e anonimizada, para aferir a adesão da população ao isolamento social.

Diante de tal cenário, surge a necessidade de se promover discussões acerca dos direitos à privacidade e à proteção de dados pessoais. A fim de contextualizar o leitor, o presente texto aborda as diferenciações entre esses dois direitos. Ademais, é traçado todo o desenvolvimento histórico legislativo até que fosse editada uma norma específica e inteiramente voltada a proteger o direito à proteção de dados pessoais: a Lei Geral de Proteção de Dados Pessoais (LGPD).

Em seguida, são apresentados ao leitor os principais aspectos da Lei, isto é, os princípios, os conceitos de maior importância, as terminologias utilizadas e as bases normativas que autorizam o tratatamento de dados pessoais.

Feita a contextualização, passa-se à situação específica do uso de dados de geolocalização durante a crise do coronavírus, especialmente, quanto aos sistemas de monitoramento implementados em São Paulo e em Recife. Nesse ponto, são propostas as seguintes questões de pesquisa: *(i)* se os dados coletados são anonimizados e agregados, há riscos à privacidade e à proteção de dados?; *(ii)* se a LGPD busca proteger o tratamento de dados de pessoas físicas e singularizadas, há a sua aplicabilidade nesses casos?; *(iii)* a legislação de proteção de dados brasileira deve ser analisada apenas sob uma perspectiva individual ou caberia também uma perspectiva coletiva?

Desse modo, para solucionar as questões de pesquisa apontadas, primeiramente, buscou-se demonstrar o poder dos algoritmos, sobretudo, para inferir perfis comportamentais a partir da coleta de dados de georreferenciamento. Logo após, são expostas ao leitor as peculiaridades que envolvem o procedimento de anonimização e a sua manifesta falibilidade. Ato contínuo, este texto passa a discutir questões afetas à agregação de dados e seus riscos à coletividade.

Por último, após algumas críticas e conclusões a todo o raciocínio traçado, a problemática da discriminação algorítmica passa a ser explorada. Por intermédio da discriminação direta ou da discriminação indireta, é demonstrado que as máquinas inteligentes podem estigmatizar indivíduos e grupos, principalmente em contextos de pandemia.

Todos os temas abordados no presente texto visam convencer o leitor acerca da importância dos direitos à privacidade e à proteção de dados, especialmente quando se considera as circunstâncias de uma crise epidemiológica, em que se difunde a falsa ideia de que saúde e proteção de dados consistem em um *trade-off*.

Com a finalidade de se alcançar os objetivos propostos, realizou-se ampla pesquisa bibliográfica e documental, além disso, foram trazidos alguns precedentes judiciais que abordam e analisam essa oportuna temática.

1. UMA BREVE CONTEXTUALIZAÇÃO: COMPREENDENDO CONCEITOS E EXPLORANDO O DESEVOLVIMENTO HISTÓRICO DA LEGISLAÇÃO

1.1 Direito à privacidade e direito à proteção de dados pessoais

O direito à privacidade e à proteção de dados pessoais com as suas atuais feições são, indubitavelmente, uma conquista histórica da sociedade e da própria democracia, uma vez que hoje representam verdadeiras ferramentas que emancipam os indivíduos.

Em 1890, Samuel Warren e Louis Brandeis formularam o célebre artigo "*The right to privacy"*, no qual se estampou as necessidades da sociedade burguesa norte-americana no final do século XIX (DONEDA, 2000, p. 2). Os citados doutrinadores empreenderam esforços em demonstrar como as fotografias instantâneas e a indústria dos jornais impressos invadiam o recinto privado e a vida doméstica (FERREIRA; RESENDE, 2021, p. 87). Desse modo, o burguês buscava a proteção de um local apenas seu, revelando uma nova necessidade de intimidade (RODOTÀ, 2008, p. 26). Assim, a privacidade consistia meramente no direito a ser deixado só, isto é, revelava um dever de abstenção que remontava ao paradigma do *zero-relationship* com a inexistência de comunicação entre um sujeito e os demais (DONEDA, 2006, p. 8).

Com o fim do patrimonialismo exacerbado e com a inserção da pessoa humana no centro do ordenamento jurídico, a privacidade, além de passar a ser um direito fundamental, na visão de Danilo Doneda, deixou de ser vista apenas sob o âmbito de uma liberdade negativa, relacionada à não ingerência externa e ao isolamento, adquirindo um elemento positivo, "indutor da cidadania" e meio necessário para a "construção e consolidação de uma esfera privada própria" (DONEDA, 2006, p. 24).

Conforme afirma Stefano Rodotà, a nova definição da privacidade envolve um papel mais ativo do indivíduo, representando seu direito de manter o controle sobre as informações concernentes a si (RODOTÀ, 1995, p. 122 *apud* DONEDA, 2006, p. 147). Portanto, nas exatas palavras de Rodotà, a privacidade passa a ser identificada como "a tutela das escolhas de vida contra toda a forma de controle público e estigmatização social" (RODOTÀ, 2008, p. 92). Em complemento a essa ideia, Gilmar Ferreira Mendes, Inocêncio Coelho e Paulo Gustavo Branco entendem que a privacidade é "condição para o livre desenvolvimento da personalidade da pessoa humana". (MENDES; COELHO; BRANCO, 2007, p. 421).

Realizada esta breve contextualização acerca da evolução do conceito de privacidade, passa-se à explanação do direito à proteção de dados, principal objeto do presente estudo.

O direito à proteção de dados surgiu em momento posterior como desdobramento do direito à privacidade. Danilo Doneda preceitua que a disciplina da proteção de dados pessoais surgiu para funcionalizar a proteção da privacidade (DONEDA, 2006, p. 27).

De igual modo, Lorenzo Dalla Corte afirma que a distinção entre privacidade e proteção de dados pessoais se dá por intermédio de um critério teleológico. A privacidade seria um direito de perfil substantivo, criado para proteger interesses considerados importantes. Por sua vez, a proteção de dados pessoais reveste-se de um caráter prevalentemente procedimental, definidor das condições mediante as quais os direitos substantivos serão implementados (CORTE, 2020, p. 41 *apud* MACHADO; MENDES, 2020, p. 116), possuindo o *télos* de "proteger as pessoas contra injustificado e abusivo tratamento e circulação de aspectos de sua personalidade" (ZANFIR, 2008, p. 245 *apud* MACHADO; MENDES, p. 117). Diego Machado e Laura Schertel Mendes ratificam o cunho procedimental do direito à proteção de dados ao afirmar que o seu intuito principal é prescrever "procedimentos e métodos a serem observados durante todo o ciclo de vida da informação pessoal" (MACHADO; MENDES, 2020, p. 116).

Por conseguinte, didaticamente, pode-se afirmar que a proteção de dados está para a privacidade assim como o direito processual está para o direito material. Em consonância com

essa ideia, Gabriela Zanfir relaciona a proteção de dados pessoais como “um direito que protege a proteção” (ZANFIR, 2008, p. 245 *apud* MACHADO; MENDES, 2020, p. 117).

Assim como a privacidade, a proteção de dados também está intimamente vinculada ao livre desenvolvimento da personalidade. O Conselho Europeu, através da Convenção de Strasbourg, em 1981, explicitou a necessária vinculação entre o direito à proteção de dados pessoais e a personalidade do indivíduo ao estabelecer o conceito de dados pessoais (EUROPA, 1981):

> Artigo 2 – Definições
>
> Para as finalidades desta Convenção:
>
> um"dado pessoal" significa qualquer informação relativa a um indivíduo identificado ou identificável ("titular dos dados").

Dessa forma, todo dado pessoal revela ou possui o potencial de revelar algo acerca da pessoa humana, consistindo em um verdadeiro atributo da personalidade. Essa premissa é ratificada por Pierre Catala, que identifica uma informação pessoal quando o objeto da informação é a própria pessoa (CATALA, 1983, p. 20, *apud* DONEDA, 2006, p. 157):

> Mesmo que a pessoa em questão não seja a ‘autora’ da informação, no sentido de sua concepção, ela é a titular legítima dos seus elementos. Seu vínculo com o indivíduo é por demais estreito para que pudesse ser de outra forma. Quando o objeto dos dados é um sujeito de direito, a informação é atributo da personalidade.

Nesta conjuntura, considerando a inequívoca importância da proteção de dados para a pessoa humana e para o ordenamento jurídico, importa salientar que, desde o ano 2000, a União Europeia trata este direito à nível constitucional, conforme previsão do artigo 8º da sua Carta de Direitos Fundamentais (UNIÃO EUROPEIA, 2000). De igual modo, analisando a regulamentação nos países da América Latina, verifica-se que, desde 1999, o Chile regulamenta a proteção de dados pessoais através de legislação específica. Países como a Argentina, o México, o Peru e a Colômbia possuem leis sobre o tema desde os anos 2000, 2010, 2011 e 2012, respectivamente (PECK, 2020). Contudo, no Brasil, a edição de uma norma direcionada à proteção de dados pessoais foi um tanto quanto tardia.

Inicialmente, verifica-se que a Constituição Federal Brasileira de 1988 inseriu a inviolabilidade da vida privada, da intimidade e do sigilo de dados no rol dos direitos fundamentais. A Carta Magna também previu o instituto do *habeas data*, um instrumento

processual para proporcionar ao cidadão o direito de acessar e de retificar seus dados armazenados em bancos públicos de dados (BRASIL, 1988).

No que diz respeito à legislação infralegal, segundo Keila Ferreira e Ana Paula Resende, a Lei nº 8.078/90, denominada Código de Defesa do Consumidor (CDC), foi por muito tempo o diploma legal que mais se aproximou da proteção de dados pessoais no ordenamento jurídico brasileiro (FERREIRA; RESENDE, 2021, p. 95). O artigo 43 do CDC merece ser destacado, uma vez que estabeleceu uma série de direitos e garantias ao consumidor referentes às suas informações pessoais constantes em cadastros e banco de dados (BRASIL, 1990).

Em 2011, foi editada pelo Congresso brasileiro a Lei de Acesso à Informação (LAI - Lei nº 12.527/2011), norma essencial que instrumentalizou e procedimentalizou os deveres de transparência e publicidade da Administração Pública perante seus administrados. A despeito de ter fixado a publicização das atividades administrativas como regra geral, a LAI previu hipóteses excepcionais às quais devem ser conferidas o sigilo. Dentre as exceções, a legislação estabeleceu em seu artigo 31 que as informações pessoais relativas à intimidade, à vida privada, à honra e à imagem devem ter seu acesso público restrito (BRASIL, 2011).

Após a Lei de Acesso à Informação, foi sancionada a Lei do Marco Civil da Internet (Lei nº 12.965/2014), legislação que primou por regulamentar o uso da internet no Brasil. O legislador inseriu a privacidade e a proteção dos dados pessoais como princípios norteadores da norma. Não há que se olvidar também que se verificou na Lei do Marco Civil inúmeros direitos e garantias aos usuários do ciberespaço brasileiro, tais como ao não fornecimento de dados pessoais a terceiros, salvo mediante consentimento livre; à prestação de informações claras e completas sobre coleta, uso, armazenamento e tratamento dos dados pessoais; e à exclusão definitiva das informações pessoais que tiverem sido fornecidas a determinada aplicação de internet, ao término da relação entre as partes (BRASIL, 2014).

Todavia, todas as legislações existentes no Brasil até então forneciam uma proteção insuficiente ao titular de informações pessoais. Tanto o CDC quanto a LAI restringiram o âmbito de incidência da proteção de dados. No caso do CDC, a lógica protetiva se limita às relações consumeristas, e, no caso da LAI, restringe-se à relação entre a Administração Pública e o administrado. Por sua vez, o instituto do *habeas data*, apesar de relevante, também se mostrou incapaz de tutelar o direito em comento, uma vez que se trata de mero instrumento processual de caráter remedial (DONEDA, 2006, p. 332). Por último, da mesma forma, a Lei do Marco Civil da Internet apenas tangenciou a temática.

Foi a partir de 2018, com a sanção da Lei Geral de Proteção de Dados Pessoais (LGPD) pelo então Presidente Michel Temer, que o Brasil deu seus primeiros passos na busca por garantir uma salvaguarda efetiva ao direito dos indivíduos à proteção de seus dados.

Em 2020, após os debates manejados pelo STF no bojo da Ação Direta de Inconstitucionalidade 6.387 e da Ação de Descumprimento de Preceito Fundamental 695, entendeu-se que o direito do indivíduo de autodeterminar seus dados pessoais tem status de direito fundamental (BRASIL, 2020). Nessa linha, em 20 de outubro de 2021, o Senado Federal aprovou a Proposta de Emenda à Constituição nº 17/2019, que tornou a proteção de dados pessoais, inclusive nos meios digitais, uma garantia constitucional, prevista no novo inciso LXXIX do artigo 5º da Constituição Federal (BRASIL, 2019).

1.2 A Lei Geral de Proteção de Dados Pessoais (LGPD)

A criação da Lei de Proteção de Dados Pessoais envolveu ampla participação de diferentes atores públicos e da sociedade civil, de modo que foram realizadas inúmeras audiências para debater a estrutura e o texto da lei. Nessa conjuntura, após longo debate, a normativa brasileira foi aprovada seis anos após o Projeto de Lei nº 4.060/2012 ter ido ao Plenário da Câmara dos Deputados (MELO; MIRANDA; TABORDA; ROHMANN, 2021, p. 6). Contudo, criada a LGPD, muito se discute acerca das motivações de sua edição e a razão de ter sido tão tardia. O contexto nacional e internacional dá indícios de que o governo brasileiro não possuía muito interesse na sua aprovação.

Com o intuito de situar o leitor acerca da falta de engajamento das autoridades brasileiras em aprovar uma lei de proteção de dados pessoais, salienta-se, inicialmente, que a coleta de informações de caráter pessoal pode ser utilizada com finalidade política. Um dos casos emblemáticos de uso político dos dados pessoais foi a estratégia utilizada pelo ex-presidente norte-americano Donald Trump na disputa das eleições de 2016. Na ocasião, a empresa *Cambridge Analytica* coletou dados pessoais fornecidos por milhões de usuários do *Facebook* em um "inofensivo" aplicativo que continha um teste de personalidade. As informações pessoais foram utilizadas para catalogar o perfil dos indivíduos e, então direcionar, de forma mais certeira, as publicidades políticas (COMO..., 2018).

Oportunamente, após o famoso caso ocorrido nos Estados Unidos, Bradshaw e Howard realizaram estudos que constatam que atores públicos utilizam estratégias tecnológicas para

manipular a opinião pública. Os pesquisadores citam que uma das formas de manipulação com uso de tecnologia é a disseminação *online* de propagandas pró-governo ou pró-partido político; de cunho difamatório para atacar a oposição; ou para conduzir uma polarização entre os cidadãos. Ademais, Bradshaw e Howard afirmam explicitamente que o Brasil figura entre os países adeptos a tal prática (BRADSHAW; HOWARD, 2019, p. 4-15).

A manipulação em massa pode ser realizada com a disseminação de desinformação, isto é, de *fake news.* Segundo Bradshaw e Howard, as autoridades públicas utilizam dados pessoais, obtidos de forma *online* e *offline*, para direcionar informações inverídicas a grupos específicos (BRADSHAW; HOWARD, 2019, p. 17). Em complemento a esse fato, Marcelo Martins e Victor Tateoki confirmam que a produção de notícias falsas tem motivação política, para "persuadir ou polarizar questões sociais relevantes para beneficiar alguém (ou algum grupo político) em futuras eleições" (MARTINS; TATEOKI, 2019, p. 142).

Com a finalidade de ilustrar tais considerações, é essencial frisar que, muito recentemente, o atual Presidente da República brasileira editou a Medida Provisória nº 1068/2021, que visava alterar a Lei do Marco Civil da Internet. Conforme afirma Laura Schertel Mendes, a MP restringiu a liberdade das plataformas digitais ao exigir a demonstração de "justa causa para a remoção de conteúdo e exclusão de contas, prevendo de forma taxativa as hipóteses que se enquadram nesse conceito". Notícias falsas, discursos de ódio e manipulação da informação não faziam parte da justa causa, por exemplo. A Medida Provisória ficou nacionalmente conhecida como *"MP das Fake News"*, uma vez que tudo indica que seu principal objetivo foi assegurar que os apoiadores pudessem ter um salvo conduto para disseminar a desinformação (LAURA..., 2021).

De forma coerente à lógica do Estado Democrático de Direito, o Presidente do Senado devolveu a Medida Provisória, alegando a sua inconstitucionalidade (PACHECO..., 2021). Além disso, por meio da Ação Direta de Inconstitucionalidade 6.991, a Ministra Rosa Weber já havia suspendido, de forma liminar, a eficácia da MP, ante à ausência dos requisitos da urgência e relevância, e pela inviabilidade de "veiculação, por meio de medida provisória, de matérias atinentes a direitos e garantias fundamentais" (BRASIL, 2021).

Assim, traçado esse panorama, é possível sustentar que a possibilidade de utilizar os dados pessoais para fins políticos como meio para disseminar *fake news* e promover a manipulação de grupos específicos da sociedade, sem a limitação de uma norma de proteção de dados, colocava as autoridades públicas brasileiras em uma situação um tanto quanto

confortável. No entanto, para além dessa tese, a necessidade de criação da LGPD surgiu diante de fatores específicos do contexto internacional.

Pode-se afirmar que a criação da Lei Geral de Proteção de Dados Pessoais foi impulsionada por dois motivos. O primeiro deles deve-se ao fato de que o governo brasileiro, há algum tempo, tenta ingressar na Organização para Cooperação e Desenvolvimento Econômico (OCDE) e um dos requisitos para ser membro é justamente a regulamentação da proteção de dados pessoais. Após a edição da LGPD, o Brasil encontra-se mais próximo de seu objetivo, haja vista que o próprio Secretário-Geral da OCDE, Angel Gurría, defendeu "a LGPD como um passo importante para aumentar a confiança na transformação digital no Brasil" (GOVERNO..., 2021).

A segunda motivação para a inserção da LGPD no ordenamento jurídico brasileiro envolve a Regulação Geral de Proteção de Dados da União Europeia (*General Data Protection Regulation* – GDPR), à qual criou obstáculos para a transferência de dados pessoais a países que não possuíssem um sistema de proteção de dados considerado adequado (MONTEIRO, 2018). Desse modo, conforme afirma Patrícia Peck, tal previsão significava que "o Estado que não possuísse lei de mesmo nível passaria a poder sofrer algum tipo de barreira econômica ou dificuldade de fazer negócios com os países da União Europeia" (PECK, 2021, p. 10). Ou seja, pode-se afirmar que o Brasil tinha receio de sofrer represálias econômicas.

Nesse viés, o Congresso brasileiro criou uma norma específica e autônoma para dispor sobre o tratamento de dados pessoais: a LGPD, fortemente inspirada na GDPR. Ambas as leis possuem bases conceitual e principiológica bem semelhantes, apesar de a normativa brasileira ser mais enxuta e menos detalhista quando comparada à regulação europeia (MALDONADO; BLUM, 2019, p. 21-22).

A Lei Geral de Proteção de Dados Pessoais brasileira define o dado pessoal de forma idêntica à definida pelo Conselho Europeu na Convenção de Strasbourg, em 1981. Em seu artigo 5º, inciso I, a LGPD conceitua dado pessoal como a "informação relacionada a pessoa natural identificada ou identificável" (BRASIL, 2018). Gustavo Gasiola, Diego Machado e Laura Schertel Mendes explanam a diferenciação entre quando a pessoa é identificada e quando é identificável (GASIOLA; MACHADO; MENDES, 2021, p. 185-186):

> Quando a pessoa natural for identificada, a relação entre a informação e a pessoa é direta, ou seja, será possível atribuir características a uma pessoa determinada, sem a necessidade de informação adicional. Quando a pessoa natural for identificável, haverá uma relação indireta entre a informação e a

> pessoa natural. Isso, porque o conteúdo da informação não é suficiente para a imputação inequívoca de uma característica a uma pessoa. Entretanto, a informação será pessoal a medida que existe potencialidade de identificação, quando combinada a outras informações.

A LGPD, assim como a maioria das normas sobre proteção de dados pessoais, diferencia os dados pessoais comuns dos dados pessoais sensíveis. Os dados pessoais serão classificados como sensíveis sempre que possuírem um potencial discriminatório e estigmatizante, facilitando processos sociais de exclusão e segregação, motivo pelo qual seu controle deve ser ainda mais rigoroso (KONDER, 2019, p. 451). A Lei indica no seu artigo 5º, inciso II, que a informação poderá ser discriminatória quando for referente à origem racial ou étnica, à convicção religiosa, à opinião política, à filiação a sindicato ou a organização de caráter religioso, filosófico ou político, à saúde ou à vida sexual, à dado genético ou biométrico, quando vinculado a uma pessoa natural (BRASIL, 2018).

Assim, pela análise dos conceitos de dados pessoais e de dados pessoais sensíveis, verifica-se que a LGPD protege os dados pessoais apenas das pessoas naturais, não abarcando as pessoas jurídicas. Todavia, não importa quem esteja realizando o tratamento de dados, todos estarão sujeitos à aplicação dessa norma, sejam pessoais naturais ou sejam pessoas jurídicas, inclusive o Poder Público, por expressa determinação do parágrafo único do artigo 1º da Lei Geral de Proteção de Dados Pessoais. Insta salientar que, conforme disposição da norma, os atores que manuseiam informações pessoais devem respeitar a Lei durante todo o ciclo de vida do dado pessoal, desde a sua coleta, transmissão e armazenamento até a sua eliminação (BRASIL, 2018).

A norma brasileira ainda prevê outra relevante distinção, dessa vez entre os dados anonimizados e os dados pseudoanonimizados, previstos no artigo 5º, inciso III, e no artigo 13, § 4º, respectivamente. Segundo Danilo Doneda, a anonimização das informações pessoais é uma técnica que quebra o vínculo entre o(s) dado(s) e seu(s) respectivo(s) titular(es) (DONEDA, 2006, p. 44), por isso, a princípio, não há que se falar em aplicabilidade da LGPD, uma vez que não se está diante de um dado que possibilita identificar ou tornar identificável o indivíduo. Por outro lado, Bruno Bioni ensina que a pseudoanonimização consiste em um método de falsa ou superficial anonimização, já que a própria organização que a empregou possui meios próprios para transmudar um dado aparentemente anonimizado em um dado pessoal (BIONI, 2020, p. 194).

No que tange à base principiológica da norma, constata-se que a Lei Brasileira é norteada por 11 (onze) princípios, incluindo o da boa-fé. Dentre os mais relevantes para o presente estudo, destaca-se *(i)* o princípio da finalidade, configurado pelo tratamento realizado com propósitos específicos e informados ao titular; *(ii)* o princípio da adequação, tida como a compatibilidade do tratamento com as finalidades que foram informadas ao titular; *(iii)* o princípio da necessidade, que consiste na limitação do tratamento ao mínimo necessário para realizar as suas finalidades; *(iv)* o princípio da transparência, que envolve o dever de disponibilizar informação clara, precisa e de fácil acesso ao titular; *(v)* o princípio da prevenção, consistente na adoção de medidas aptas a prevenir a ocorrência de danos advindos do tratamento; *(vi)* o princípio da não discriminação, o qual impossibilita a realização de tratamento com fins discriminatórios ilícitos e abusivos; e *(vii)* o princípio da responsabilização e prestação de contas, configurada como a demonstração, pelo controlador de dados, de medidas hábeis a comprovar a observância e o cumprimento das normas de proteção de dados pessoais (RODRIGUES; FERREIRA, 2019, p. 196).

Para além dos conceitos e princípios, a LGPD também seguiu o exemplo europeu ao criar uma Autoridade Nacional de Proteção de Dados Pessoais (ANPD), responsável por emitir recomendações e pareceres técnicos, além de fiscalizar todas as entidades que manuseiam dados pessoais, possuindo, inclusive, atribuição para aplicar-lhes sanções (RODRIGUES; FERREIRA, 2019, p. 196-198). Todavia, a lei brasileira divergiu da maioria das normas estrangeiras em um aspecto: no primeiro momento, a LGPD não conferiu à ANPD plena independência, de modo que a Autoridade estava vinculada à Presidência da República. Laura Schertel Mendes e Danilo Doneda afirmam que o Brasil fazia parte de um seleto grupo de países que não constituiu uma autoridade independente (MENDES; DONEDA, 2018, p. 478), por isso, Graham Greenleaf chega a afirmar que essas nações "são conhecidas internacionalmente como parte de um pequeno corredor da vergonha" (GREENLEAF, 2017 *apud* MENDES; DONEDA, 2018, 478).

Contudo, apesar das críticas à falta de uma Autoridade Nacional de Proteção de Dados autônoma, alguns estudiosos defendiam a ideia de que sequer seria necessária a implementação de uma Autoridade aos moldes da experiência internacional. Rafael Pellon e Flavia Lefèvre sugeriram que seria muito benéfico que o Conselho Administrativo de Defesa Econômica (CADE) incorporasse a responsabilidade pela execução da política pública de proteção de informações pessoais, uma vez que *(i)* os direitos da concorrência e o da proteção de dados estão intimamente interligados; *(ii)* a incorporação da ANPD ao CADE oneraria bem menos os

cofres públicos; e *(iii)* a operacionalização seria bem mais ágil, pois se aproveitaria uma estrutura e um corpo técnico robustos e já consolidados (ANPD..., 2020). No entanto, a despeito da divergência de pensamentos, o certo é que a Autoridade de Proteção de Dados já está em atividade e, recentemente, após a publicação da Medida Provisória 1.124 de 13 de junho de 2022, tornou-se uma autarquia de natureza especial (MEDIDA..., 2022).

Há que se destacar que um outro ponto de convergência da LGPD com as leis estrangeiras é que o tratamento de dados não poderá ser realizado sem que haja uma base normativa que o autorize (MENDES; DONEDA, 2018, p. 472). Dentre as 10 (dez) hipóteses legais autorizadoras do tratamento de informações pessoais, dispostas no artigo 7º, estão o consentimento, ou seja, a manifestação livre e intencional pela qual o titular concorda com o tratamento de seus dados; a proteção da vida ou da incolumidade física do titular ou de terceiro; o cumprimento de obrigação legal ou regulatória; e o legítimo interesse do controlador dos dados. No que tange ao tratamento de dados pessoais sensíveis, a Lei restringiu as bases normativas ao rol do artigo 11 (BRASIL, 2018).

A LGPD preocupou-se em direcionar bases legais especificamente para a Administração Pública, dispondo em seu artigo 7º, inciso III, e seu artigo 23, dois suportes normativos: a execução de políticas públicas e a realização de competências administrativas ou atribuições legais de serviço público (BRASIL, 2018). Ainda no âmbito do Poder Público, a Lei demonstrou expressamente a legalidade em se compartilhar dados pessoais entre os diferentes órgãos da Administração, desde que sejam respeitados todos os princípios elencados no artigo 6º (RODRIGUES; FERREIRA, 2019, p. 136).

Foi em 2020, com o surgimento da fatídica pandemia da COVID-19, que o Poder Público utilizou e compartilhou constantemente os dados pessoais como forma de combate ao coronavírus, porém, sem parâmetro limitador, uma vez que a LGPD ainda se encontrava em período de *vacatio legis.*

1.3 A Administração Pública Digital: os dados e o vírus

Não obstante o presente artigo tenha um recorte extremamente atual, salienta-se que, conforme José Sérgio Cristóvam e Tatiana Hahn afirmam, há registros de que, desde o século XVI, a Administração Pública coleta dados pessoais dos seus administrados. No Brasil, o

primeiro órgão a coletar informações pessoais para finalidade estatística foi a Diretoria Geral de Estatística, ainda na época do Império, em 1871 (CRISTÓVAM; HAHN, 2020, p. 5).

Tais fatos revelam que o tratamento de informações pessoais sempre foi atividade inerente à gestão pública, seja para fins de atuação do Estado nas áreas de defesa nacional e saúde, seja para a coleta de informações estatísticas em tópicos sociais (CRISTÓVAM; HAHN, 2020, p. 5). Vinícius Oliveira, sabiamente, aduz que "o Poder Público, sem dados, é como uma cuia que nada acondiciona, e que, portanto, propósito nenhum serve" (OLIVEIRA, 2021, p. 19). Não é à toa que José Sérgio Cristóvam e Tatiana Hahn utilizam a expressão "Administração Pública orientada por dados" (CRISTÓVAM; HAHN, 2020, p. 1).

Com o advento da Quarta Revolução Industrial e com o consequente desenvolvimento tecnológico, foi preciso repensar o Estado na Era Digital. José Luiz Faleiros Júnior afirma que a Administração Pública passou por reformas estruturais para se adequar à nova fase comunicacional, denominada de "sociedade da era da informação". A reformulação foi tamanha que até do ponto de vista terminológico houve alterações: os doutrinadores passaram a intitular a Administração de "Digital", utilizando o prefixo *"e"* para se referir a aspectos do governo, tais como os vocábulos estrangeiros *e-government*, *e-governance* e *e-democracy* (FALEIROS JÚNIOR, 2020, p. 11).

Como forma de melhoria da eficiência e de eficácia, a Administração Pública Digital passou a tratar os dados pessoais de forma automatizada e massiva, de forma que, nas palavras de José Sérgio Cristóvam e de Tatiana Hahn, tornou-se "uma das maiores detentoras de dados no mundo" (CRISTÓVAM; HAHN, 2020, p. 4). Não é coincidência que hoje o *big data* público é uma realidade.

No cenário de pandemia mundial instaurada pela COVID-19, a Administração Pública também utilizou amplamente os dados pessoais, "seja para fins de modelar e executar políticas públicas de contenção e controle do vírus, seja para tornar possível que pesquisas científicas proporcionem os melhores resultados possíveis no menor tempo", conforme aduzem Daniela Cravo e Marcela Joelsons (CRAVO; JOELSONS, p. 112).

A necessidade do uso de dados pessoais como medida de enfrentamento de crises epidemiológicas alcançou certo consenso após os surtos dos vírus Ebola e Zika entre 2015 e 2016, uma vez que se considerou que "o acesso amplo e rápido de informações seria essencial para os pesquisadores produzirem conhecimento científico relevante para orientar a tomada de

decisões de governos e autoridades sanitárias no enfrentamento de epidemias" (MACHADO; MENDES, 2020, p. 106).

Com o intuito de ratificar a importância do tratamento de dados pessoais em contexto de crises sanitárias, ressalta-se que o Comitê Europeu para a Proteção de Dados, no documento de Diretrizes nº 4/2020, sublinhou que o quadro de normas que versam sobre a proteção de dados pessoais foi concebido para ser flexível e, como tal, suscetível de dar uma resposta eficaz no que se refere à limitação da pandemia (UNIÃO EUROPEIA, 2020). De igual modo, Danilo Doneda afirma que, em situações de emergência, a sociedade deve utilizar os dados pessoais sempre que puderem ser úteis (DONEDA, 2020).

No âmbito nacional, verifica-se que o tratamento de dados pessoais como forma de combate ao coronavírus foi realmente utilizado. A Associação *Data Privacy* Brasil de Pesquisa criou o projeto "Dados Virais" com a finalidade de mapear as tecnologias digitais baseadas no uso de dados pessoais adotadas durante a pandemia da COVID-19. Conforme o estudo, apurou-se 253 (duzentos e cinquenta e três) casos de iniciativas dos governos municipais, estaduais e federal para enfrentamento da calamidade pública. Assim como o Brasil, inúmeros países valeram-se de estratégias tecnológicas para a condução de políticas públicas efetivas durante o período de crise epidemiológica (DATA PRIVACY BRASIL, 2021).

Os dados de geolocalização estão entre os mais utilizados pela Administração Pública como instrumento de enfrentamento do coronavírus. As tecnologias empregadas permitiram o monitoramento *on-line* em massa da população de países de todas as partes do mundo (CRAVO; JOELSONS, 2020, p. 116).

Taiwan é um dos casos emblemáticos do uso da tecnologia da geolocalização para rastreamento. De acordo com o que narram Rafael Zanatta, Bruno Bioni, Clara Keller e Iasmine Favaro, depois que três mil pessoas desembarcaram de um navio e, em seguida, algumas testaram positivo para a COVID-19, o governo de Taiwan utilizou os dados de geolocalização individuais para procurar eventuais contatos entre seus cidadãos e passageiros (ZANATTA; BIONI; KELLER; FAVARO, 2020, p. 235).

Os mesmos escritores descrevem que a Noruega também utilizou essa tecnologia, visto que adotou um sistema que realizava o rastreamento ao vivo da geolocalização dos indivíduos (ZANATTA; BIONI; KELLER; FAVARO, 2020, p. 235).

Daniela Cravo e Marcela Joelsons relatam outro famoso caso de vigilância, dessa vez na China (CRAVO; JOELSONS, 2020, p. 116):

> Na China, a população deve utilizar um aplicativo de celular desenvolvido para detectar a exposição ao vírus e classificar a população com base no histórico de deslocamento e condições de saúde, que gera um código QR em uma das três cores. Um código verde permite que seu portador se mova sem restrições. Alguém com um código amarelo pode ser solicitado a ficar em casa por sete dias. Vermelho significa quarentena de duas semanas. Além disso, toda vez que o código de uma pessoa é verificado - em um posto de saúde -, por exemplo -, sua localização atual parece ser enviada aos servidores do sistema, o que permite às autoridades rastrear os movimentos das pessoas ao longo do tempo.

No Brasil, o monitoramento por meio da geolocalização, em alguns casos, foi feito por meio de parcerias com as empresas de telecomunicações, às quais possuem a tecnologia necessária para entender o comportamento de localização dos usuários (CRAVO; JOELSONS, 2020, p. 117).

Em São Paulo, os dados são fornecidos ao governo pelas empresas de telefonia Vivo, Claro, Oi e Tim, baseados no sinal emitido pelas antenas de celular. As informações são organizadas em gráficos e mapas, atualizados diariamente, os quais demonstram o índice de adesão ao isolamento social. No sítio eletrônico do Governo do Estado de São Paulo, é possível verificar que é formado um *ranking* que classifica os municípios por ordem dos que mais aderem ao isolamento até os que menos aderem. Os dados de geolocalização são obtidos de forma agregada e anonimizada, ou seja, à princípio, não são capazes de serem vinculados a uma pessoa determinada (SP..., 2022).

Em Recife, as autoridades também têm acesso ao mapeamento de aglomerações pela geolocalização dos *smartphones*, através da tecnologia fornecida pela empresa *In Loco*. Os dados obtidos geram um índice de isolamento por bairro. E, caso necessário, os gestores enviam carros de som para os locais onde há maior aglutinação de pessoas (PREFEITURA..., 2020). Assim como no caso de São Paulo, os dados utilizados são agregados e anonimizados (CRAVO; JOELSONS, 2020, p. 118).

No entanto, há que se salientar que, apesar de o tratamento de informações pessoais ser necessário à contenção de pandemias, “a legitimação para o seu uso em situações de emergência não é, de forma alguma, uma carta em branco fornecida pelas legislações de proteção de dados para o emprego irrestrito de dados pessoais”, é o que alerta Danilo Doneda (DONEDA, 2020).

Nesse sentido, analisando os casos de utilização de dados de geolocalização, acima expostos, questiona-se se o direito à privacidade e a à proteção de dados pessoais, especialmente os parâmetros delineados pela LGPD, foram e estão sendo, de fato, respeitados.

2 O USO DE DADOS DE GEOLOCALIZAÇÃO DURANTE A PANDEMIA DA COVID-19

2.1 A importância dos dados de geolocalização e as técnicas aplicadas

A coleta de dados de geolocalização, quando analisada isolada e superficialmente, pode parecer inofensiva e incapaz de violar qualquer direito do indivíduo (CRAVO; JOELSONS, 2020, p. 119). Todavia, em análise mais minuciosa, verifica-se que o uso de informações de georreferenciamento, principalmente quando se considera o contexto de uma pandemia, pode indicar uma hipervigilância do titular de dados ou, como Yuval Harari alerta, uma vigilância totalitária (HARARI, 2020).

A GDPR, diferentemente da LGPD, mencionou explicitamente os dados de geolocalização para exemplificar o conceito de dados pessoais. O artigo 4º do Regulamento de Proteção de Dados da União Europeia conceitua que uma informação é considerada pessoal quando revela a identidade do indivíduo ou, ao menos, torna possível a identificação. Desse modo "é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo, dados de localização" (UNIÃO EUROPEIA, 2016).

A preocupação da GDPR em fazer menção aos dados de georreferenciamento não é mero acaso. Atualmente, os dados de geolocalização são extremamente valiosos para as grandes empresas. A título exemplificativo, Bruno Bioni aduz que o monitoramento da localização geográfica é uma estratégia para direcionar a publicidade. Assim, "leva-se em conta a proximidade física do potencial consumidor com o bem ofertado", ou seja, não é uma mera coincidência que "surja um anúncio publicitário, cujo bem de consumo esteja bem próximo ao cidadão" (BIONI, 2021, p. 20).

Não há que se olvidar também que os dados de georreferenciamento podem ser considerados como "dados observados". Conforme ensinam Sergio Negri, Maria Regina

Korkmaz e Elora Fernandes, a OCDE categorizou os dados de acordo com a sua origem. O dado será "observado" quando "advindo da fruição ou interação do usuário com a plataforma digital, como, por exemplo, a geolocalização do usuário" (NEGRI; KORKMAZ; FERNANDES, 2021, p. 9). Ou seja, o dado de geolocalização será classificado como observado quando a sua coleta for pressuposto para o uso de certos aplicativos, como por exemplo, o *Waze* e o *Google Maps*.

Sobre esta temática, Anderson de Paiva e Ivana David alertam que inúmeros *apps* instalados nos *smartphones* coletam e armazenam silenciosamente, sem qualquer consentimento, os dados de geolocalização através do *GPS* (Sistema de Posicionamento Global) e, como se não bastasse, vendem-os a terceiros (GABRIEL; DAVID, 2020).

Gustavo Vieira traz outro interessante caso em que se usa dados de georreferenciamento como estratégia de grandes companhias: a avaliação de riscos, no caso específico da securitização de veículos. A localização em tempo real dos motoristas permite ao algoritmo mapear as probabilidades de furtos e acidentes veiculares, sendo possível alcançar um valor do prêmio securitário proporcional à possibilidade de se ocorrer um sinistro (VIEIRA, 2019, p. 66).

Desse modo, os inúmeros exemplos de uso de dados de georreferenciamento revelam a sua importância para as grandes empresas, mas, principalmente, indicam a potencialidade de identificação do titular desses dados.

Ter conhecimento da localização do indivíduo permite ao algoritmo inferir suas características e seus gostos pessoais. Isto é, se a pessoa frequenta certas espécies de restaurante, infere-se o seu gosto gastronômico; se o indivíduo se localiza com frequência em certo templo ou igreja, a inteligência artificial faz inferências sobre a sua orientação religiosa; se a pessoa frequenta uma universidade, infere-se que assuntos acadêmicos são de seu interesse.

A OCDE denomina esse tipo de informação de dado inferido, isto é, "o produto de processos analíticos baseados em probabilidade", que torna viável a realização de correlações para criar previsões de comportamento, utilizadas para categorizar o indivíduo (ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT, 2014). Assim, correlacionar um conjunto de dados permite ao algoritmo inferir a própria personalidade do titular de dados. Este procedimento de inferências para a construção de perfis refere-se à tecnologia intitulada de perfilamento. Francesca Bosco ensina a conceituação dessa técnica (BOSCO, 2017):

> Perfilamento é uma técnica de tratamento (parcialmente) automatizado de dados pessoais e/ou não pessoais, que visa a produção de conhecimento por meio da inferência de correlações de dados na forma de perfis que podem ser posteriormente aplicados como base para a tomada de decisão.

Assim, não é à toa que os algoritmos agem com cada vez mais acurácia, realizando anúncios publicitários e ofertando produtos direcionados e personalizados para atender cada perfil. O agir preciso das ferramentas algorítmicas ocasiona, em um primeiro momento, certo fascínio, uma vez que as técnicas computacionais geram a impressão de que a máquina conhece intimamente o ser humano. Essa tecnologia é tão impactante que o legislador, na edição da LGPD, preocupou-se em inseri-la em disposição específica (BRASIL, 2018):

> Art. 12. § 2º Poderão ser igualmente considerados como dados pessoais, para os fins desta Lei, aqueles utilizados para formação do perfil comportamental de determinada pessoa natural, se identificada.

Diego Machado e Laura Schertel Mendes aduzem que as novas tecnologias que utilizam métodos preditivos ameaçam a violação dos direitos à proteção de dados pessoais e à privacidade. Ao inferir as preferências e vontades humanas, o algoritmo passa a conduzir a pessoa e interferir na sua própria identidade, uma vez que as ferramentas computacionais são capazes de gerar uma confusão no titular de dados: torna-se dificultoso diferenciar o que é a sua personalidade real e genuína do que é a sua personalidade inferida e atribuída pela máquina. Assim, " a pessoa passa a agir sem sequer ter certeza de que se conduz de acordo com os seus próprios desejos e predileções" (MACHADO; MENDES, 2020, p. 126).

Por conseguinte, o risco ao direito à proteção de dados pessoais reside no fato de que é tirado dos titulares dos dados a "capacidade de uso de mecanismos de controle do tratamento automatizado de suas informações e contestação das decisões que afetam seus direitos e interesses". De igual modo, o direito à privacidade também é colocado em xeque, uma vez que, "o processo de construção da identidade passa a sofrer interferências de agentes artificiais que podem atuar com base numa equivocada representação da pessoa" (MACHADO; MENDES, 2020, p. 127).

Quando se considera o tratamento de dados de geolocalização durante a pandemia da COVID-19, a lógica não é muito distinta à retratada. Conforme Diego Machado, Laura Schertel Mendes e Sean McDonald ressaltam, o emprego de dados de localização de dispositivos de telefonia móvel para conhecer padrões de mobilidade de indivíduos e de grupos são de extrema

relevância durante todo o ciclo de vida da pandemia para que os entes públicos entendam a distribuição geográfica das infecções do coronavírus e, a partir daí, tomem as decisões e avaliem as intervenções em matéria de saúde pública. (MCDONALD, 2016, p. 12 *apud* MACHADO; MENDES, 2020, p. 110).

Os casos já mencionados de São Paulo e de Recife captam uma atenção maior, já que o tratamento de dados de georreferenciamento é feito de forma anonimizada e baseado em estatística agregada (MACHADO; MENDES, 2020, p. 112), com o intuito de criar mapas de calor e índices de isolamento social por região monitorada, como mecanismo de contenção da crise epidemiológica.

Esse cenário traz relevantes questionamentos: se os dados são anonimizados e agregados, isto é, se não identificam uma pessoa singular, há riscos à privacidade e à proteção de dados? Se a LGPD busca proteger o tratamento de dados de pessoas físicas e singularizadas, há a sua aplicabilidade nesses casos? As respostas não são simples nem muito menos pacíficas.

A empresa *In Loco*, que auxiliou as autoridades públicas recifenses a mapear as aglomerações, não foi alvo de debates judiciais para se questionar eventual violação aos direitos da proteção de dados pessoais e da privacidade. Em 2018, o Ministério Público do Distrito Federal e Territórios havia instaurado inquérito civil para investigar a obtenção de dados pessoais de brasileiros por essa *startup*. Contudo, após meses de análises, a investigação restou arquivada, uma vez que se entendeu que, por não haver coleta de dados que permita a vinculação direta ao titular dos dados pessoais, o "modelo de negócio está em conformidade com a legislação vigente" (MEDEIROS, 2020 *apud* ZANATTA; BIONI; KELLER; FAVARO, p. 239).

Por sua vez, a legalidade do Sistema de Monitoramento Inteligente, implementado pelo governo paulista, foi apreciada pela Ministra do STJ Laurita Vaz, que entendeu que não havia qualquer risco ou ferimento do direito à privacidade, tampouco perigo ou restrição à liberdade de locomoção, uma vez que a análise de dados não se dá de modo individualizado e as informações são observadas de forma aglutinada (ZANATTA; BIONI; KELLER; FAVARO, 2020, p. 244):

> No que concerne à presente deliberação, o que há de concreto é que tanto o Governo estadual, como as operadoras de telefonia celular, esclarecem que no sistema implementado os usuários não são especificadamente individualizados. Como consequência disso, tem-se que o habeas corpus coletivo ora manejado mostra-se incabível também em razão de não ter sido demonstrada a possibilidade de identificação dos alegadamente atingidos (BRASIL, 2020).

Todavia, antes de qualquer conclusão, deve-se analisar de forma mais aprofundada as peculiaridades da anonimização e da agregação de dados.

2.2 A anonimização

Logo no início da pandemia da COVID-19, em 21 de abril de 2020, o Comitê Europeu para a Proteção de Dados adotou diretrizes para estabelecer as condições da utilização de dados de georreferenciamento para controlar a propagação do vírus (Diretrizes 4/2020). Dentre as recomendações, foi destacado que deve ser "sempre dada preferência ao tratamento de dados anonimizados em vez de dados pessoais" (UNIÃO EUROPEIA, 2020).

Antônio Houaiss e Mauro de Salles Villar afirmam que a antítese do conceito de dado pessoal seria um dado anônimo, ou seja, aquele que é incapaz de revelar a identidade da pessoa (HOUAISS; VILLAR, 2009, p. 140 *apud* BIONI, 2020, p. 191). No artigo 12, a LGPD salienta a exclusão dos dados anonimizados do âmbito de aplicação da norma (BRASIL, 2018).

No entanto, Bruno Bioni ressalta que o processo de anonimização é algo tão falível (BIONI, 2020, p. 191), de modo que retirar os vínculos de identificação de uma base de dados com 100% (cem por cento) de eficiência pode ser considerado um mito (NARAYANAN; SHMATIKOV, 2010, p. 24 *apud* BIONI, 2020, p. 191). Considerando essa lógica, Omer Tene conclui que "qualquer dado pessoal anonimizado detém o risco inerente de ser transmudado em um dado pessoal" (TENE, 2013, p. 1242).

Contudo, conforme alerta Bruno Bioni, esse raciocínio pode levar a uma redundância normativa, já que os dados anonimizados seriam sempre, em última análise, informações relacionadas a uma pessoa identificável. Por isso, deve-se adotar um teste de razoabilidade para delimitar a fronteira entre dado anonimizado e dado pessoal. (BIONI, 2020, p. 192). A própria LGPD trouxe a previsão desse teste da razoabilidade em seu artigo 12, *caput*, e § 1º (BRASIL, 2018).

Segundo a lei de proteção de dados brasileira e conforme esclarecem Bruno Bioni, José Luiz Faleiros Júnior e Guilherme Martins, há dois eixos para se analisar a razoabilidade: *(i)* um objetivo, que analisa o custo e o tempo necessários para reverter o processo de anonimização (FALEIROS JÚNIOR; MARTINS, 2021, p. 389); e *(ii)* um subjetivo, que considera quem é o

controlador de dados e se ele dispõe de meios próprios para reverter o processo de anonimização (BIONI, 2020, p. 194).

Desse modo, pela simples exposição dos critérios da razoabilidade, observa-se um certo subjetivismo, uma vez que a LGPD deixou uma ampla margem de discricionariedade para se avaliar o grau de reversibilidade de um dado anonimizado. Bruno Bioni aduz que tal análise tem caráter eminentemente circunstancial, ou seja, os dois eixos de estudo, tanto o objetivo quanto o subjetivo, "ganharão vida apenas a partir do contexto no qual está inserida uma atividade de tratamento de dados" (BIONI, 2020, p. 197).

Considerando a conjuntura da pandemia da COVID-19, mais especificamente, nos casos dos governos de São Paulo e de Recife, que obtiveram acesso aos dados de geolocalização anonimizados através das parcerias com operadoras de telefonia e com a *startup In Loco*, respectivamente, verifica-se que há indícios de que a nebulosa anonimização pode ter sido utilizada como escudo contra questionamentos (FALEIROS JÚNIOR, 2020). Isto é, as empresas e as autoridades públicas podem ter se valido do subjetivismo da anonimização para evitar ao máximo discussões sobre eventual violação aos direitos da privacidade e da proteção de dados.

No que tange ao eixo objetivo da análise do critério da razoabilidade, constata-se que para as operadoras de telefonia, para os órgãos públicos e para a *startup In Loco* pode não ser tão moroso e custoso reverter um processo de anonimização. De igual modo, no que se refere ao critério subjetivo do teste da razoabilidade, há indícios de que esses agentes detêm os meios próprios para viabilizar a reidentificação.

Anderson de Paiva e Ivana David refletem que "observar um ponto anonimizado movendo-se pelo mapa ao longo de uma semana, muitas vezes, revela onde essa pessoa mora, trabalha e costuma fazer suas refeições" (GABRIEL; DAVID, 2020). Ademais, através da técnica do perfilamento, outros atributos pessoais podem vir a ser inferidos, facilitando a reidentificação do indivíduo. Diego Machado e Laura Schertel Mendes defendem que esses "ataques inferenciais" atualmente podem configurar meios e exigir esforços não razoáveis para identificar titulares de dados (MACHADO; MENDES, 2020, p. 141).

Além disso, conforme Ira Rubistein e Woodrow Hartzog afirmam, há fatores de risco e de mitigação para se analisar o grau de reversibilidade do dado anonimizado. Dentre os fatores de risco, destaca-se o volume de dados, ou seja, "quanto maior a quantidade de dados, maiores são as chances de alguém fazer o caminho inverso de um processo de anonimização". Assim,

os autores afirmam que modelos de negócios e políticas públicas “que envolvam grandes massas de dados devem proporcionalmente apresentar técnicas de anonimização correspondentes aos altos riscos de reidentificação" (RUBINSTEIN; HARTZOG, 2015 *apud* BIONI, 2020, p. 197).

O tratamento massivo de dados é um fator de risco que se amolda exatamente ao caso da coleta de dados de georreferenciamento durante a crise epidemiológica advinda do coronavírus. Segundo a Associação *Data Privacy* Brasil de Pesquisa, mais de 30.000 (trinta mil) celulares dos habitantes paulistas estariam sendo monitorados. Em Recife, esse número ultrapassa os 700.000 (setecentos mil) (DATA PRIVACY BRASIL, 2020, p. 65).

Ira Rubistein e Woodrow Hartzog apontam outro fator que aumenta as chances de transmudar um dado anonimizado em um dado pessoal: a complexidade da cadeia da atividade de tratamento de dados. Assim sendo, “quanto maior for o ingresso de entidades para a geração ou o uso de uma base de dados anonimizada, mais elevado será o risco de reidentificação, uma vez que não se aumenta apenas o volume do fluxo informacional, como, também, a população que dele participa (RUBINSTEIN; HARTZOG, 2015 *apud* BIONI, 2020, p. 197).

Volvendo à análise da utilização de dados de geolocalização durante a pandemia da COVID-19, verifica-se que, no curso da crise viral, foi editada a Lei nº 13.979/2020, que tornou obrigatório o compartilhamento de dados pessoais, entre órgãos e entidades da administração pública, das pessoas infectadas ou com suspeita de infecção pelo coronavírus (BRASIL, 2020). Essa disposição legal já revela que o compartilhamento de dados durante esse período foi intenso.

Um compartilhamento seguro pressupõe uma adequada governança de dados durante todo o ciclo de vida do dado, desde a sua coleta até o seu descarte. Carlos Barbieri ensina que a governança de dados envolve “gerência informacional; melhoria na valoração e produção dos dados; monitoração de seu uso, além de aspectos críticos de segurança, privacidade, ética e aderência a regras de *compliance*”. Para tanto, devem ser adotadas políticas e diretrizes corporativas para que os dados sejam tratados com responsabilidade (BARBIERI; 2020, p. 36). Cumpre salientar que uma boa governança de dados deve ser adotada inclusive para dados anonimizados, que, à princípio, não são pessoais. Assim, os riscos de reidentificação estariam mitigados.

Contudo, as entidades públicas não vêm adotando uma governança de dados adequada. O Tribunal de Contas da União, em parceria com a Secretaria de Fiscalização de Tecnologia da

Informação, instaurou a Auditoria 039.606/2020-1 para traçar um diagnóstico do grau de implementação da LGPD no âmbito da Administração Pública Federal. O Órgão de Contas avaliou 382 (trezentos e oitenta e dois) órgãos públicos, dentre eles a Secretaria-Executiva do Ministério da Saúde. O relatório, disponibilizado em 15 de junho de 2022, revelou resultados alarmantes. Em metodologia de autoavaliação, apenas 34% (trinta e quatro por cento) das organizações afirmaram que todos os compartilhamentos de dados estão em conformidade com os critérios estabelecidos na LGPD. No que se refere à adoção de parâmetros de segurança de dados, 84% (oitenta e quatro por cento) dos órgãos não possuem plano de respostas a incidentes que abrange o tratamento de incidentes de violação de dados pessoais. Em conclusão, o Relator afirma que 76,7% (setenta e seis vírgula sete por cento) das entidades estão no grau inexpressivo ou inicial do processo de adequação à norma de proteção de dados (BRASIL, 2022).

De igual modo, as empresas de telefonia, que realizam o monitoramento da localização geográfica através das ferramentas disponíveis nos *smartphones*, tais como o *GPS* e o *Bluetooth*, parecem também não ter uma boa política de governança de dados. A despeito da Lei Geral de Telecomunicações (Lei nº 9.472/1997) garantir o direito do usuário ao respeito à sua privacidade (BRASIL, 1997), verifica-se que a realidade é outra: as operadoras de telefonia repassam indiscriminadamente os dados pessoais de seus clientes a terceiros.

A título exemplificativo, ilustra-se que, no ano de 2022, o Ministério Público do Estado da Bahia ajuizou ações civis contra a Vivo, Oi, Tim e Claro, em razão do compartilhamento indevido de dados e consequente violação à privacidade dos consumidores. Na investigação das referidas ações, a Agência Nacional de Telecomunicações (ANATEL) comprovou que as "operadoras não vêm agindo em conformidade com as regras destinadas à proteção dos dados pessoais, acarretando o ilícito compartilhamento dos dados, bem como diversos danos" (MP..., 2022).

Portanto, os fatos relatados parecem comprovar que a rede de controladores de dados, no contexto da pandemia, foi complexa, uma vez que diversos terceiros provavelmente ingressaram no fluxo informacional e cruzaram esse banco anonimizado de dados com outros bancos, sem o respaldo de uma adequada governança de dados.

Ademais, há que se destacar que, no caso de São Paulo, não foi sequer divulgada a técnica de anonimização que está sendo utilizada nem muito menos as técnicas preventivas contra eventual vazamento de dados (FALEIROS JÚNIOR, 2020), o que demonstra um desrespeito ao princípio da transparência, previsto na LGPD. Outro fator agravante é que não

foi elaborado um relatório prévio de impacto à proteção de dados pessoais, contrariando os parâmetros de prevenção e de responsabilização impostos pela Lei.

Assim, conforme aduz José Luiz Faleiros Júnior, “ainda que louvável, o Sistema de Monitoramento Inteligente paulista é falho em sua gênese”, ante à ausência de transparência e à total inexistência de uma *accountability* (FALEIROS JÚNIOR, 2020). Tais omissões devem-se também ao fato de que à época da implantação desses sistemas de rastreio de *smartphones* para controlar o coronavírus, a LGPD não estava em vigor para balizá-los.

Logo, na conjuntura da pandemia da COVID-19, a tecnologia do perfilamento, o volume de dados tratados e os intensos e indiscriminados compartilhamento e cruzamento de dados fragilizam e representam riscos ao procedimento da anonimização. Somado a esses fatores, a ausência de transparência quanto à técnica utilizada e de parâmetros de uma adequada governança de dados corroboram a tese de que os dados anonimizados de geolocalização podem ser facilmente revertidos em dados pessoais, viabilizando a reidentificação dos indivíduos. Considerando tal premissa, não haveria que se falar, portanto, em anonimização, mas sim em uma pseudoanonimização, que atrairia a aplicação da LGPD.

Ultrapassada a questão da anonimização propriamente dita, outro importante fator que merece ser analisado na conjuntura da pandemia é a questão da aglutinação dos dados de georreferenciamento.

2.3 A agregação de dados e a dimensão coletiva do direito à privacidade e à proteção de dados pessoais

O Sistema de Monitoramento Inteligente, implementado pelo Estado de São Paulo, disponibiliza o índice de isolamento social de cada município. No caso de Recife, a *In Loco* utiliza ferramentas de geolocalização que monitoram cada bairro recifense. Em que pese não haver identificação de uma pessoa singular, há a identificação de grupos. Ou seja, apesar de não ser possível identificar qual indivíduo está descumprindo as regras de isolamento, é possível identificar qual município/bairro está.

Sobre essas considerações, Diego Machado e Laura Schertel Mendes esclarecem, oportunamente, que as discussões atuais sobre a privacidade e a proteção de dados pessoais consideram a sua dimensão coletiva, ou seja, esses direitos merecem ser tutelados não apenas

de forma individual, como também transindividual. Nesse sentido, não há que se confundir o interesse coletivo com o somatório dos interesses dos indivíduos que integram o grupo (MACHADO; MENDES, 2020. p. 126).

Edward Bloustein e Alessandro Mantelero destacam que a privacidade de grupo se distingue da privacidade coletiva. A privacidade do grupo é "um atributo dos indivíduos em associação uns com os outros", assim o interesse protegido é o desejo e a necessidade das pessoas de se reunirem, trocarem informações e compartilharem sentimentos" (BLOUSTEIN, 2017). Por outro lado, a privacidade coletiva, diferentemente da privacidade de grupo, "não considera apenas a agregação de interesses individuais, mas também diferentes interesses específicos voltados para o próprio grupo e não para cada um de seus membros" (MANTELERO, 2017).

Considerando tais premissas, salienta-se que todas as tecnologias de geolocalização aplicadas a uma pessoa singularizada, também podem se aplicar a uma coletividade. Diego Machado e Laura Schertel Mendes aduzem que as técnicas de perfilamento são aplicáveis aos grupos, intitulando-se de *group profiling* (MACHADO; MENDES, 2020, p. 122-123). Isto é, a partir do processo de produção de conhecimento das máquinas mediante probabilidades e inferências, pode-se criar tanto um perfil individual, como um perfil do grupo.

A segmentação de um grupo de consumidores, levando em conta a sua localização geográfica, é uma ferramenta estratégica para as empresas fornecerem publicidade direcionada. A partir do *group profiling*, as preferências de um grupo que reside em certa localidade são inferidas. Assim, há certos anúncios publicitários que nunca vão ser direcionados a uma coletividade residente em uma região, mas que sempre serão direcionados a outro grupo localizado em região distinta.

Não há que se olvidar também que inúmeras práticas discriminatórias são praticadas a nível coletivo, "de forma que a individualização de um titular de dados tem pouca relevância em certos tipos de contexto" (MACHADO; MENDES, 2020, p. 127). A título exemplificativo, cita-se o fato de que a observação do padrão de mobilidade de um grupo e de sua adesão ao isolamento social pode permitir perigosas inferências sobre focos de futuras doenças epidemiológicas (MACHADO; MENDES, 2020, p. 124). Para ilustrar tal situação, imagine o seguinte cenário: com o surgimento de uma nova pandemia, as autoridades públicas recifenses e paulistas inferem, a partir dos dados coletados na crise da COVID-19, quais regiões geográficas não seguirão as recomendações de isolamento social, e, por isso, estabelecem,

desde logo, intervenções mais severas nesses locais. Imaginar futuros panoramas ocasiona, no mínimo, certa intriga, por isso, a discriminação com base em dados de geolocalização é um tema de grande relevo que será detalhado no próximo capítulo.

Por conseguinte, a agregação de dados pode ser considerada uma verdadeira "faca de dois gumes". Em que pese, tenha como objetivo resguardar os direitos individuais do indivíduo, põe em risco os direitos dos grupos.

Nessa conjuntura, a Lei de Telecomunicações, ao prever, em seu artigo 72, § 2°, que "a prestadora poderá divulgar a terceiros informações agregadas sobre o uso de seus serviços, desde que elas não permitam a identificação, direta ou indireta, do usuário, ou a violação de sua intimidade" (BRASIL, 1997), desconsidera que a própria agregação já pode representar riscos.

Assim, muito embora a finalidade precípua da LGPD seja proteger pessoas naturais e singularizadas, a própria lei indica uma possível expansão normativa para se considerar também uma proteção a grupos, principalmente quando se observa o seu artigo 22 (BRASIL, 2018):

> Art. 22. A defesa dos interesses e dos direitos dos titulares de dados poderá ser exercida em juízo, individual ou coletivamente, na forma do disposto na legislação pertinente, acerca dos instrumentos de tutela individual e coletiva.

Diego Machado e Laura Schertel Mendes afirmam que a interpretação sistemática da LGPD, a fim de salvaguardar a dimensão coletiva da norma, "parece ser a única consistente com a proteção e promoção de direitos e liberdades fundamentais" (MACHADO; MENDES, 2020, p. 137). Ademais, a Lei deve seguir a lógica do próprio ordenamento jurídico, considerando que as legislações têm resguardado a tutela coletiva de direitos. Cita-se o Código de Defesa do Consumidor, que equipara a figura do consumidor à coletividade de pessoas, ainda que indetermináveis (BRASIL, 1990); e a norma que disciplina a Ação Civil Pública, que protege "qualquer interesse difuso ou coletivo" (BRASIL, 1985).

Portanto, em breve síntese, os sistemas de monitoramento implementados durante a pandemia da COVID-19, quando examinados sob o aspecto da dimensão individual ou coletiva, possivelmente possuem desdobramentos lesivos ao direito à proteção de dados pessoais e à privacidade (MACHADO; MENDES, 2020, p. 141). Conforme será observado nos próximos tópicos, esse cenário parece se agravar ainda mais quando se analisam *(i)* o potencial discriminatório do uso de dados de geolocalização; e *(ii)* o risco das medidas de vigilância se normalizarem e se perpetuarem.

3. A PANDEMIA DA COVID-19 E OS DADOS DE GEOLOCALIZAÇÃO: UM OLHAR PARA O FUTURO

3.1 A discriminação algorítmica

As decisões humanas estão sendo progressivamente terceirizadas a sistemas de inteligência artificial, uma vez que, supostamente, as falibilidades e as limitações das máquinas são menores (FRAZÃO, 2022, p. 1). Todavia, até que ponto as decisões automatizadas são neutras e desprovidas de subjetivismo? Ben Green e Lily Hu alertam que as preocupações dos agentes privados e públicos com a acurácia e com a eficiência dos dados se sobrepõem a questões relacionadas à justiça e à igualdade (GREEN; HU, 2018, p. 1). Nessa conjuntura, faz-se necessário analisar brevemente o processo de tomada de decisão dos algoritmos inteligentes.

O perfilamento e os demais métodos inferenciais baseados em probabilidade são realizados em três etapas: *(i)* a inserção de dados (*input*); *(ii)* o tratamento; e *(iii)* a emissão de dados (*output*) (DUARTE; NEGÓCIO, 2021, p. 226). A fase de inserção de dados normalmente é executada pelo próprio programa computacional a partir de um banco de dados pré-existente. Desse modo, os dados gerados nos *outputs* se tornarão futuros dados a serem utilizados nos *inputs*. Ou seja, a máquina funciona através de um sistema de retroalimentação, de modo que quanto maior a quantidade de operações, maior é a sua base de dados e, consequentemente, maior é a sua eficiência nas tarefas preditivas. A partir daí, surge o conceito do *machine learning*, isto é, o sistema adquire autonomia e passa a tomar decisões automatizadas através de seu próprio processo de aprendizagem.

Nesses processos, os algoritmos inteligentes, muitas vezes, "absorvem padrões discriminatórios presentes na sociedade e replicam como se fossem uma verdade objetiva" (MENDES; MATTIUZZO, 2019, p. 41). Assim, a qualidade dos dados inseridos nos *inputs* é questionável, uma vez que o indivíduo que inicialmente programou o sistema pode ter tido a intenção de gerar resultados estigmatizantes. Nesse caso, em que há a intencionalidade, fala-se em discriminação direta (MOREIRA, 2017, p. 17 *apud* DUARTE; NEGÓCIO, 2021, p. 224).

Todavia, independentemente da qualidade do *input*, pode-se gerar resultados discriminatórios a partir da correlação de dados (MENDES; MATTIUZZO, 2019, p. 41).

Alexander Tischbirek ratifica essa ideia ao afirmar que “a discriminação está não só na causalidade, mas também nas correlações” (TISCHBIREK, 2019 *apud* DUARTE; NEGÓCIO, 2021, p. 224). Nessa conjuntura, fala-se em discriminação indireta, isto é, “a desigualdade de resultados causada pelo uso de um critério neutro” (JUNQUEIRA, 2020, p. 92).

Além de poder ser classificada como direta ou indireta, a discriminação algorítmica pode atingir tanto uma pessoa singularizada, quanto um grupo. No que tange especificamente à discriminação de uma coletividade, Alan Duarte e Ramon de Vasconcelos afirmam que os algoritmos carregam subjetivismos e crenças que podem levar a uma tomada de decisão que promova a exclusão de um determinado grupo (DUARTE; NEGÓCIO, 2021, p. 220). Em complemento a essa premissa, Laura Schertel Mendes e Marcela Mattiuzzo destacam que os algoritmos se baseiam, na maioria das vezes, em discriminação estatística, fundada na probabilidade de tal grupo agir de determinada maneira (MENDES; MATTIUZZO, 2019, p. 41).

Feitos tais apontamentos, quando se trata especificamente dos dados de geolocalização, verifica-se que uns dos grandes exemplos de discriminação algorítmica estão materializados nas práticas denominadas de *geopricing* e *geoblocking*. No caso do *geopricing*, empresas como companhias aéreas e agências de viagens cobram preços distintos por um mesmo produto ou serviço a depender da localização geográfica do indivíduo. Ou, no caso do *geoblocking*, as informações são manipuladas de tal forma que, para um certo grupo de uma determinada localidade, o *site* ou o aplicativo revela que há indisponibilidade de vagas ou que certo serviço ou produto inexiste, contudo, para outro grupo de outra região, a informação revelada é exatamente oposta. A título ilustrativo, cita-se que um caso famoso de *geopricing* foi praticado pela companhia de turismo e hospedagem “Decolam.com”. Na ocasião, a Secretaria Nacional do Consumidor (Senacon) aplicou à empresa multa de 2,5 (dois vírgula cinco) milhões por oferecer diferentes preços para reservas em hotéis no Brasil, de acordo com o país do consumidor (DECOLAR..., 2022).

Sob outro viés, quando se examina o uso dos dados de georreferenciamento no contexto da crise do coronavírus, observa-se que existem indícios de que práticas discriminatórias foram, estão sendo e poderão ser praticadas contra determinados grupos. Uma evidência disso é que, desde o início da pandemia, as autoridades mundiais de saúde se preocupam com possíveis discriminações atreladas às regiões geográficas acometidas (BRUNS; KRAGULJAC; BRUNS, 2020).

Nessa conjuntura, destaca-se que a descoberta da COVID-19 na China, no ano de 2019, trouxe estigmas para a população chinesa. Terminologias como “vírus chinês” e “vírus asiático” foram utilizadas no início da pandemia como forma de discriminar os chineses e, até mesmo, responsabilizá-los pelo surgimento da crise epidemiológica (BORGES et al., 2021, p. 2). A discriminação contra a China foi agravada pela disseminação de inúmeras *fake news*, dentre elas, a de que o coronavírus seria o resultado de um experimento para desenvolver uma arma biológica (CHINA..., 2021).

Ato contínuo, o coronavírus passou a estar atrelado às regiões geográficas com maior concentração de renda, uma vez que esses grupos, que possuem poder aquisitivo para viajar para países estrangeiros, contaminaram-se com a COVID-19, que até então não circulava no Brasil. Para ilustrar tal fato, cita-se que, em abril de 2020, as autoridades públicas da cidade de Recife constataram que o bairro com mais casos de coronavírus era justamente o luxuoso bairro de Boa Viagem, na Zona Sul (BOA..., 2020). Assim, a mídia passou a estigmatizar essas coletividades, utilizando o termo “a doença dos ricos” e responsabilizando-as por terem propagado o vírus pelo país (CORONAVÍRUS..., 2020).

Em um terceiro momento, após a implementação das medidas governamentais contra a propagação do vírus, surgiram as tecnologias que aferem os índices de isolamento social de cada bairro/município, através da geolocalização dos *smartphones*. Esses sistemas inteligentes, sobretudo o de São Paulo e o de Recife, revelaram que as regiões geográficas que mais respeitaram a quarentena são as que possuem baixo número de habitantes. De acordo com o sítio eletrônico do Governo do Estado de São Paulo, o município de São Joaquim da Barra ocupa a primeira posição no ranking de aderência ao isolamento social (SP..., 2022). Já em Recife, o bairro de Paissandu foi o mais adepto à quarentena (VEJA..., 2020). Por outro lado, localidades com maior número de moradores e situados geograficamente no centro das metrópoles são os que apresentaram maiores graus de aglomeração (ISOLAMENTO..., 2020).

Nesse viés, a informação incluída no banco de dados das máquinas inteligentes foi a de que grupos menores respeitam medidas de enfrentamento à COVID-19 mais do que grupos maiores. Assim, em uma eventual e futura nova pandemia, ocasionada por outro vírus, os algoritmos podem inferir que, como grupos maiores tiveram menor adesão à quarentena na ocasião do coronavírus, também terão o mesmo padrão de comportamento em um contexto de outro agente viral.

Todavia, é razoável concluir que todos os grupos maiores são menos adeptos a medidas preventivas contra agentes virais? De igual modo, é aceitável inferir que o comportamento de um grupo na ocasião de uma pandemia será repetido em uma eventual próxima crise? O que se pretende alertar através dessas reflexões é que tais generalizações poderão dar ensejo a práticas discriminatórias.

De acordo com o que afirma Thiago Junqueira, a generalização é exatamente um dos caminhos que levam à discriminação (JUNQUEIRA, 2020, p. 15). Laura Schertel Mendes e Marcela Mattiuzzo aduzem que a denominada discriminação por generalização ocorre quando "pessoas são equivocadamente classificadas em certos grupos" (MENDES; MATTIUZZO, 2019, p. 52). Em analogia, é possível concluir que se indivíduos são erroneamente inseridos em certas coletividades, alguns subgrupos também podem ser equivocadamente inseridos em um grupo que não lhes representa.

Imagine a injustiça que se cometeria caso, em uma eventual nova crise epidemiológica, bairros/municípios com maior quantidade de moradores fossem desde logo tachados de não serem adeptos a medidas de isolamento social. Tal estigmatização poderia até mesmo fazer com que autoridades públicas aumentassem de imediato a vigilância nessas regiões geográficas.

Logo, em que pese os algoritmos inteligentes serem de grande valia para uma eficiente tomada de decisão no âmbito dos poderes público e privado, deve-se ater ao fato de que dados de geolocalização, utilizados nos contextos de pandemia, podem levar a injustas estigmatizações, de modo que não deve ser desconsiderada sua potencialidade discriminatória e, portanto, seu grau de sensibilidade.

Feitas essas considerações, passa-se ao último tópico, no qual serão analisados os riscos de as medidas ostensivas de vigilância perdurarem ao longo do tempo, bem como possíveis soluções para evitar o denominado uso secundário de dados.

3.2 O dataísmo e as lições para o mundo pós-coronavírus

Conforme demonstrado acima, a inteligência artificial, além de replicar crenças e preconceitos presentes na sociedade, realiza inferências injustas que podem estigmatizar determinados grupos. No entanto, muitos indivíduos não percebem tal realidade, uma vez que

já foi depositada tanta confiança nos algoritmos que hoje se tornou difícil desmistificar certas ideias.

Com o intuito de ilustrar o poder dos dados, Yuval Harari afirma que os indivíduos passaram a crer cegamente nos algoritmos, isto é, colocou-se fé no *big data*, de modo que hoje se pode falar em uma nova religião intitulada de dataísmo, em que os dados possuem valor intrínseco e incontestável (HARARI, 2016).

A crença nos dados se torna mais fervorosa nos contextos de pandemia, uma vez que as medidas de vigilância passaram a ser sempre justificadas em prol de bens maiores: a saúde e a vida (HARARI, 2020). Ou seja, os dados passaram a ser vistos como verdadeiros "salvadores da pátria".

Assim, com a finalidade de garantir que não houvesse contestação às novas tecnologias adotadas, disseminou-se a falsa ideia de que privacidade e saúde são excludentes entre si, consistindo em um *trade-off*. Por isso, os indivíduos foram inconscientemente obrigados a tomar uma escolha, que, nesse caso, foi pela saúde, com o intuito de vencer a pandemia do coronavírus (HARARI, 2020, p. 35-36).

Ou seja, as autoridades públicas disseminam falsas ideias a fim de que a sociedade perca cada vez mais a capacidade de questionar criticamente a tecnologia e a tomada de decisão dos governos e dos algoritmos inteligentes: como é feito o monitoramento? Qual é a finalidade da medida? Por quanto tempo ocorrerá a vigilância?

A perda da criticidade leva os sujeitos a um verdadeiro estado de manipulação, de modo que não há mais reflexões acerca dos malefícios que uma coleta incessante de dados pode trazer à privacidade e à proteção de dados pessoais dos indivíduos. Pelo contrário, o senso popular se restringe a pensar que quanto mais dados são coletados, mais efetiva será a gestão pública. Assim, sem qualquer exame crítico, transparência ou possibilidade de contestação efetiva, a inteligência artificial, com apoio das autoridades públicas, subjuga por completo as pessoas (FRAZÃO, 2021, p. 2).

Nesse contexto, Yuval Harari afirma que os governos famintos por dados podem utilizar qualquer pretexto para manter os sistemas de monitoramento em funcionamento, seja pelo mero temor de uma quarta onda de casos de coronavírus, seja porque há uma nova cepa de ebola na África Central (HARARI, 2020, p. 35).

O que se teme é que as autoridades públicas ludibriem as pessoas e as convençam de que o sistema de monitoramento é importante para controlar a propagação de determinado agente viral. Há que se alertar que esse cenário pode não estar tão distante, uma vez que, atualmente, a doença denominada de "varíola dos macacos", em que pese ter sido declarada muito menos transmissível e letal do que quando comparada à COVID-19 (VARÍOLA..., 2022), pode ser utilizada como uma justificativa para a manutenção das tecnologias de monitoramento, mesmo que não seja necessária.

Desse modo, com o intuito de evitar vigilâncias perpétuas e a consequente criação de um "governo todo-poderoso" (HARARI, 2020), deve-se ter uma análise mais atenta à própria LGPD a fim de que os indivíduos possam ter consciência acerca dos limites do uso dos dados de geolocalização coletados durante a pandemia da COVID-19 e, assim, possam se empoderar e cobrar posicionamentos mais assertivos da ANPD.

De início, ressalta-se que a coleta de tais dados foi legal, uma vez que se justifica através das bases legais previstas na Lei Geral de Proteção de Dados Pessoais. Conforme o Guia Orientativo emitido pela Autoridade Nacional de Proteção de Dados, o tratamento de dados pessoais pelo Poder Público é autorizado por meio do *(i)* consentimento; *(ii)* legítimo interesse; *(iii)* cumprimento de obrigação legal ou regulatória; ou *(iv)* execução de políticas públicas (AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS, 2022).

No caso do consentimento, verifica-se que ao coletar dados de georreferenciamento, através dos sinais emitidos pelos *smartphones*, não houve qualquer autorização manifesta e inequívoca do titular de dados. Quanto ao legítimo interesse, a ANPD pondera que essa hipótese deve ser utilizada de forma residual pelo Poder Público, não sendo "apropriada quando o tratamento de dados pessoais é realizado de forma compulsória ou quando for necessário para o cumprimento de obrigações e atribuições legais do Poder Público" (AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS, 2022, p. 9).

Excluídas as duas primeiras bases legais, pode-se afirmar que a coleta de dados de geolocalização durante a crise do coronavírus se justifica pelas outras duas hipóteses. Quanto à base legal do "cumprimento de obrigação legal", verifica-se que o Poder Público tinha a incumbência de adotar medidas para conter a propagação do vírus, uma vez que garantir a saúde dos indivíduos é um de seus deveres. Ademais, quanto à hipótese legal da "execução de políticas públicas", observa-se que o enfrentamento do coronavírus envolveu um conjunto de

ações organizadas e previstas em legislação própria - Lei nº 13.979/2020 - ou seja, combater o agente viral consistiu em uma verdadeira política pública.

A despeito da ANPD não ter referenciado a base legal da "proteção da vida ou da incolumidade física do titular ou de terceiro" para quando o controlador de dados for o Poder Público, Mario Viola e Chiara Teffé entendem que a aplicação dessa hipótese "poderia ser para o tratamento de dados importantes com a finalidade de se conter o avanço de epidemias, como o recente caso da COVID-19" (VIOLA; TEFFÉ, 2021, p. 137).

Portanto, justificado o tratamento dos dados de geolocalização por pelo menos três bases legais, importa salientar que, em homenagem ao princípio da finalidade, foi informado que o intuito da coleta de tais dados era aferir a adesão ao isolamento social como forma de orientar a tomada de decisão das autoridades públicas no combate ao coronavírus.

A questão cinge-se justamente nesse ponto. O objetivo específico da coleta desses dados foi o enfrentamento da COVID-19. Assim, caso o sistema de vigilância ostensiva perdure mesmo após o fim do coronavírus, o princípio da finalidade restaria desvirtuado. Miriam Wimmer denomina tal fenômeno de uso secundário de dados, isto é, "a utilização de dados para finalidades distintas daquelas que justificaram a sua coleta original" (WIMMER, 2021, p. 1).

Wimmer ensina que o uso secundário de dados é excepcionalmente permitido, desde que haja uma compatibilidade entre as finalidades (WIMMER, 2021, p. 7). Assim, em que pese haver um certo grau de subjetivismo no conceito de compatibilidade (WIMMER, 2021, p. 5), entende-se que não é razoável nem proporcional considerar um tratamento adicional desses dados para outra finalidade que não seja a de enfrentamento do coronavírus.

Conforme demonstrado no tópico anterior, a discriminação algorítmica ocasionada por generalizações e inferências injustas gera estigmas a determinados grupos, de modo que eventual uso secundário de dados poderia criar novas situações de estigmatizações. Observar o padrão de deslocamento geográfico de certa coletividade pode ensejar nefastas consequências. Imagine um cenário (não tão hipotético) de autoritarismo e regime de exceção no qual tal sistema de monitoramento é utilizado para perseguir determinados grupos.

Ou seja, quando se trata de tratamento de dados, o princípio da finalidade específica ganha um especial relevo principalmente como forma de proteger o titular de dados. Assim, eventuais tentativas de perpetuar as medidas ostensivas de vigilância dos cidadãos não se justificam e devem ser prontamente rechaçadas.

Além da análise acerca das bases legais e do uso secundário de dados, outro fator que os indivíduos devem estar atentos para minimizar a subjugação pelas máquinas inteligentes é que, além da necessidade de haver uma espécie de auditoria humana para revisar as decisões automatizadas - artigo 20 da LGPD - deve ser assegurado o "direito de como ser visto" (WACHTER; MITTELSTADT, 2019, p. 496-498). Para evitar a formação de perfis equivocados, que porventura possam prejudicar os titulares de dados, propõe-se que, no processo de inferências, o controlador deve se sujeitar a uma justificativa *ex ante* e *ex post* (JUNQUEIRA, 2020, p. 350).

Thiago Junqueira afirma que a justificativa *ex ante* corresponde ao exame de questões importantes tais como: *(i)* se os dados "seriam relevantes para se extraírem inferências; *(ii)* o porquê de as inferências extraídas serem relevantes para o fim almejado; e *(iii)* se os dados e métodos estatísticos utilizados seriam adequados" (JUNQUEIRA, 2020, p. 350-351). Por sua vez, a justificativa *ex post* configura-se no direito do titular de dados de "contestar eventual inferência imprecisa e irrazoável" (JUNQUEIRA, 2020, p. 351).

Visando ainda evitar a discriminação algorítmica, não se pode olvidar que a lógica de controlar *inputs*, dispostas nas legislações de proteção de dados, não se mostra suficiente para proteger os indivíduos e os grupos contra processos discriminatórios, uma vez que a discriminação indireta, pouco explorada na literatura e na jurisprudência, pode ocasionar predições lesivas e estigmatizantes.

Ainda, outros dois fatores críticos que impedem a LGPD de prevenir adequadamente a ocorrência de danos e os processos discriminatórios são *(i)* a falta de uma previsão clara e expressa da norma acerca da sua aplicabilidade nos casos em que há uma identificação de grupos e não de pessoas singularizadas; e *(ii)* não considerar o potencial discriminatório de dados que não são expressamente qualificados como sensíveis.

Portanto, com os apontamentos e as reflexões realizados no presente texto, caso uma nova pandemia assole o país, com as lições aprendidas através da experiência vivenciada no período da COVID-19, espera-se que a sociedade tenha mais condições de analisar com criticidade o impacto lesivo que os sistemas de monitoramento em massa podem gerar aos seus direitos à privacidade e à proteção de dados pessoais. Com essa tomada de consciência, eventuais tentativas de perpetuar as tecnologias de vigilância serão no mínimo questionadas e, ainda, posicionamentos mais incisivos e assertivos da Autoridade Nacional de Proteção de Dados poderão ser cobrados.

CONSIDERAÇÕES FINAIS

Eventos de grande magnitude, como é o caso da crise do coronavírus, trazem à tona discussões acerca dos parâmetros e das peculiaridades que envolvem os direitos à privacidade e à proteção de dados pessoais.

Com o cenário da pandemia da COVID-19, os governos fizeram e ainda fazem intenso uso de meios tecnológicos para conter o vírus, sobretudo através de sistemas de monitoramento que coletam dados de geolocalização. Contudo, no início da crise, não havia no Brasil uma legislação de proteção de dados em vigor, nem muito menos um órgão específico que balizasse, regulasse e fiscalizasse o uso de tais sistemas.

Conforme apontado, há indícios de que o surgimento tardio da LGPD pode estar ligado ao fato de que o governo brasileiro não priorizava questões afetas à privacidade e a proteção de dados pessoais. Na verdade, pode-se afirmar que há sinais de que não havia interesse de se criar uma legislação protetiva de dados pessoais, uma vez que o uso indiscriminado de informações de caráter pessoal facilitava o uso dos dados para fins políticos, sobretudo para a disseminação das *fake news* e para a consequente manipulação dos eleitores.

Para além das críticas feitas ao atraso na edição da LGPD, o presente texto ressaltou a ampla participação da sociedade civil na construção da lei, como forma de se alcançar uma redação final coerente e que oportunizasse um efetivo exercício do direito à proteção de dados.

No entanto, com o surgimento da crise da COVID-19 e com o consequente uso de sistemas de monitoramento em massa, a LGPD se mostrou omissa e insuficiente em alguns pontos.

Considerando que, no Brasil, a coleta dos dados de geolocalização, para fins de aferição do nível de adesão ao isolamento social, foi feita de forma anonimizada e agregada, assumiu-se que não havia aplicabilidade da LGPD.

Todavia, de acordo com o racicícinio traçado, não há que se falar em anonimização, mas sim em pseudoanomização, já que há claros indícios de que o dado anonimizado pode ser transmudado em dado pessoal, em razão *(i)* do enorme volume de dados, que por si só, aumenta os riscos de reindetificação; *(ii)* do intenso compartilhamento e cruzamento de dados que houve nesse período; e *(iii)* da ausência de uma adequada governança de dados. Portanto, a despeito de a Lei ter deixado ampla margem de subjetivismos para se interpretar os parâmetros do teste

de razoabilidade, conclui-se que, no caso dos sistemas de monitoramento utilizados no contexto de pandemia, o processo de anonimização pode ser facilmente revertido, atraindo a aplicabilidade da legislação de proteção de dados.

Ademais, quanto ao aspecto da agregação de dados, apesar de não haver a identificação de uma pessoa singularizada, há a identificação de grupos. Assim, em que pese ainda não haver um posicionamento assertivo da jurisprudência e da própria ANPD, além da ausência de clareza da LGPD quanto à possibilidade de se tutelar coletivamente o direito à proteção de dados, deve-se considerar a privacidade e a proteção de dados pessoais tanto em uma dimensão individual quanto em uma dimensão coletiva, em nome da coesão do ordenamento jurídico e de uma adequada proteção aos direitos fundamentais.

Outro fator que merece relevo é a potencialidade discriminatória dos dados de geolocalização, principalmente quando se considera futuros cenários de uma nova crise epidemiológica. Desse modo, a despeito de a Lei de Proteção de Dados Pessoais brasileira não qualificar os dados de geolocalização como dados sensíveis, não se pode olvidar que tais dados possuem a plena capacidade de estigmatizar indivíduos e coletividades.

Tal potencialidade discriminatória se deve ao fato de que o próprio algoritmo carrega em si crenças e preconceitos, seja pela intencionalidade do indivíduo que programou o sistema computacional, seja pela correlação de dados que gera discriminações indiretas.

Contudo, apesar de todos os possíveis desdobramentos lesivos que os sistemas de monitoramento podem gerar aos direitos à privacidade e à proteção de dados pessoais, o que mais espanta é que grande parte dos indivíduos foram meros espectadores nesse cenário de vigilância, uma vez que não criticaram nem ao menos questionaram a tentativa do governo de se tornar um verdadeiro “todo-poderoso”.

Por conseguinte, diante todo o exposto, anseia-se que a Autoridade Nacional de Proteção de Dados tenha efetivo funcionamento, isto é, fiscalize com rigor as entidades que realizam tratamento de dados; intensifique seu papel normativo; e, principalmente, seja mais ativa e incisiva em futuros e eventuais cenários de crises epidemiológicas, em que haverá um inevitável uso de dados pessoais. Ademais, espera-se que os Tribunais pátrios enfrentem e deliberem cada vez mais litígios relacionados à correta aplicação da LGPD. Por fim, após os indivíduos tomarem efetiva consciência acerca da importância do direito à proteção de dados pessoais, almeja-se que, em um futuro próximo, possa haver uma verdadeira “cultura de proteção de dados” no Brasil.

REFERÊNCIAS

ANPD no Cade: especialistas veem com bons olhos. **Teletime**, 2020. Disponível em: https://teletime.com.br/19/08/2020/anpd-no-cade-especialistas-veem-com-bons-olhos/?amp. Acesso em: 04 set. 2022.

BARBIERI, Carlos. **Governança de dados**: práticas, conceitos e novos caminhos. Rio de Janeiro: Alta Books, 2020.

BIONI, Bruno Ricardo. Compreendendo o conceito de anonimização e dado anonimizado. **Cadernos Jurídicos**, São Paulo, ano 21, n. 53, p. 191-201, jan./mar. 2020.

BIONI, Bruno. **Proteção de dados pessoais**: a função e os limites do consentimento. 3. ed. Rio de Janeiro: Forense, 2021.

BLOUSTEIN, Edward J. **Individual & Group Privacy**. Boca Raton: Routledge, 2017.

BOA Viagem e Torre lideram confirmações de coronavírus no Recife; veja lista de bairros. **G1 Globo**, 2020. Disponível em: https://g1.globo.com/pe/pernambuco/noticia/2020/04/07/veja-quais-sao-os-bairros-em-que-ha-casos-do-novo-coronavirus-no-recife.ghtml. Acesso em: 01 set. 2022.

BORGES, Tyciana Paolilo; SCHULZ, Renata da Silva; MAGALHÃES, Júlia Barbosa de; CAMPOS, Luana Moura; ANJOS, Karla Ferraz dos; ROSA, Darci de Oliveira Santa. Estigmas relacionados à COVID-19 e sua prevenção. **Physis:** Revista de Saúde Coletiva, Rio de Janeiro, v. 31, n. 1, 2021.

BOSCO, Francesca et al. Profiling technologies and fundamental rights: an introduction. *In:* CREEMERS, Niklas et al. **Profiling Technologies in Practice**: Applications and Impact on Fundamental Rights and Values. Oisterwijk: Wolf Legal Publishers, 2017. p. 9.

BRADSHAW, Samantha; HOWARD, Phillip N. The Global Desinformation Order: 2019 Global Inventory of organised social media manipulation. **University of Oxford**, 2019. Disponível em: https://digitalcommons.unl.edu/cgi/viewcontent.cgi?article=1209&context=scholcom. Acesso em: 04 set. 2022.

BRASIL. Autoridade Nacional de Proteção de Dados. **Guia orientativo**: tratamento de dados pessoais pelo Poder Público. Brasil: Autoridade Nacional de Proteção de Dados, jan. 2022. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-poder-publico-anpd-versao-final.pdf. Acesso em: 01 set. 2022.

BRASIL. **Lei nº 8.078, de 11 de setembro de 1990**. Dispõe sobre a proteção do consumidor e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/L8078compilado.htm. Acesso em: 04 set. 2022.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988**. 5 out. 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 04 set. 2022.

BRASIL. **Lei nº 7.347, de 24 de julho de 1985**. Disciplina a ação civil pública de responsabilidade por danos causados ao meio-ambiente, ao consumidor, a bens e direitos de valor artístico, estético, histórico, turístico e paisagístico e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l7347orig.htm. Acesso em: 04 set. 2022.

BRASIL. **Lei nº 9.472, de 16 de julho de 1997**. Dispõe sobre a organização dos serviços de telecomunicações, a criação e funcionamento de um órgão regulador e outros aspectos institucionais, nos termos da Emenda Constitucional nº 8, de 1995. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9472.htm#:~:text=LEI%20N%C2%BA%209.472%2C%20DE%2016%20DE%20JULHO%20DE%201997.&text=Disp%C3%B5e%20sobre%20a%20organiza%C3%A7%C3%A3o%20dos,Constitucional%20n%C2%BA%208%2C%20de%201995.&text=Art. Acesso em: 04 set. 2022.

BRASIL. **Lei nº 12.527, de 18 de novembro de 2011**. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 04 set. 2022.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. 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: 04 set. 2022.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 02 set. 2022.

BRASIL. **Lei nº 13.979, de 6 de fevereiro de 2020**. Dispõe sobre as medidas para enfrentamento de emergência de saúde pública de importância internacional decorrente do coronavírus responsável pelo surto de 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/l13979.htm. Acesso em: 04 set. 2022.

BRASIL. Senado Federal. **Proposta de Emenda à Constituição nº 17, de 2019**. Acrescenta o inciso X/1-A, ao art. 5~ e o inciso XXX, ao art. 22, da Constituição Federal para incluir a proteção de dados pessoais entre os direitos fundamentais do cidadão e fixar a competência privativa da União para legislar sobre a matéria. Brasília: Senado Federal, 2019. Disponível em: https://legis.senado.leg.br/sdleg-getter/documento?dm=7925004&ts=1647518557360&disposition=inline. Acesso em: 04 set. 2022.

BRASIL. Supremo Tribunal Federal. (Tribunal Pleno) Ação Direta de Inconstitucionalidade. **ADI 6387 MC-Ref**. 1. Decorrências dos direitos da personalidade, o respeito à privacidade e à autodeterminação informativa foram positivados, no art. 2º, I e II, da Lei nº 13.709/2018

(Lei Geral de Proteção de Dados Pessoais), como fundamentos específicos da disciplina da proteção de dados pessoais. 2. Na medida em que relacionados à identificação – efetiva ou potencial – de pessoa natural, o tratamento e a manipulação de dados pessoais hão de observar os limites delineados pelo âmbito de proteção das cláusulas constitucionais assecuratórias da liberdade individual (art. 5º, caput), da privacidade e do livre desenvolvimento da personalidade (art. 5º, X e XII), sob pena de lesão a esses direitos. O compartilhamento, com ente público, de dados pessoais custodiados por concessionária de serviço público há de assegurar mecanismos de proteção e segurança desses dados [...]. Requerente: Conselho Federal da Ordem dos Advogados do Brasil – CFOAB. Relator (a): Min. Rosa Weber. Brasília, 7 maio 2020. Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=754357629. Acesso em: 04 set. 2022.

BRASIL. Supremo Tribunal Federal. Ação Direta de Inconstitucionalidade. **ADI 6991 MC**. 1. A Emenda Constitucional 32/2001 promoveu substancial alteração no instituto da medida provisória, passando a vedar, expressamente, a sua reedição, dispondo sobre o rito procedimental para aprovação e pré-excluindo determinadas matérias do âmbito temático de tais atos normativos [...]. Requerente: Partido Socialista Brasileiro – PSB. Relator (a): Min. Rosa Weber. Brasília, 14 set. 2021. Disponível em: https://portal.stf.jus.br/processos/downloadPeca.asp?id=15347792736&ext=.pdf. Acesso em: 04 set. 2022.

BRASIL. Supremo Tribunal Federal. Arguição de Descumprimento de Preceito Fundamental. **ADPF 695 MC**. Requerente: Partido Socialista Brasileiro – PSB. Relator (a): Min. Gilmar Mendes. Brasília, 24 de junho de 2020. Disponível em: https://portal.stf.jus.br/processos/downloadPeca.asp?id=15343579920&ext=.pdf. Acesso em: 04 set. 2022.

BRASIL. Superior Tribunal de Justiça. Habeas Corpus. **HC 572996/SP**. Habeas Corpus coletivo, em que se indica como impetrado o governador do Estado de São Paulo e como pacientes os moradores da referida unidade da federação. Pretendida suspensão do Sistema de Monitoramento Inteligente (SIMI-SP), implementado em parceria do governo local com operadores de telefonia celular, para monitoração, por via de georreferenciamento, da taxa de isolamento social no Estado. Não indicação de restrição objetiva ao *jus ambulandi*. Remédio heroico: via processual destinada a tutelar apenas imediato constrangimento ilegal ao direito de liberdade. Impossibilidade de manejo de *writ* coletivo em que a parte impetrante não demonstra a possibilidade de identificação dos alegadamente atingidos. Inviabilidade, ainda, de impetração de *mandamus* contra ato em tese. Impropriedade absoluta. Petição inicial indeferida liminarmente. Impetrante: André Gustavo Zanoni Braga de Castro. Impetrado: Governador do Estado de São Paulo. Paciente: todos os moradores do Estado de São Paulo. Relator (a): Min. Laurita Vaz. Brasília, 16 de abril de 2020. Disponível em: https://processo.stj.jus.br/processo/revista/documento/mediado/?componente=MON&sequencial=108566392&num_registro=202000861909&data=20200417&tipo=0. Acesso em: 03 set. 2022.

BRASIL. Tribunal de Contas da União. Relatório de Auditoria. **TC 039.606/2020-1**. Auditoria. Diagnóstico do grau de implementação da Lei Geral de Proteção de Dados na Administração Pública Federal. 382 organizações avaliadas. Nove dimensões: preparação, contexto organizacional, liderança, capacitação, conformidade do tratamento, direitos do titular, compartilhamento de dados pessoais, violação de dados pessoais e medidas de

proteção. Maior parte das organizações em estágio inicial. Estrutura da Autoridade Nacional de Proteção de Dados. Recomendações. Entidades: Advocacia-Geral da União, Agência Brasileira de Desenvolvimento Industrial, Agência Brasileira de Inteligência, Agência Brasileira de Promoção de Exportações e Investimentos e outros. Relator (a): Min. Augusto Nardes. Disponível em: https://capitaldigital.com.br/wp-content/uploads/2022/06/038.172-2019-4-AN-auditoria_Lei-Geral-de-Protecao-de-Dados.pdf. Acesso em: 04 set. 2022.

BRUNS, D. P.; KRAGULJAC, N. V.; BRUNS, T. R. COVID-19: facts, cultural considerations, and risk of stigmatization. **Journal of Transcultural Nursing**, Estados Unidos, v. 31, n. 4, p. 326-332, 2020.

CHINA não criou coronavírus como arma biológica, diz relatório dos EUA. **Poder 360**, 2021. Disponível em: https://www.poder360.com.br/coronavirus/china-nao-criou-coronavirus-como-arma-biologica-diz-relatorio-dos-eua/. Acesso em: 01 set. 2022.

COMO os dados de milhões de usuários do Facebook foram usados na campanha de Trump. **BBC News Brasil**, 2018. Disponível em: https://www.bbc.com/portuguese/geral-43705839. Acesso em: 04 set. 2022.

CORONAVÍRUS: as doenças dos ricos matam os pobres – de vírus ou de fome. **Brasil de Fato**, 2020. Disponível em: https://www.brasildefato.com.br/2020/03/13/artigo-coronavirus-as-doencas-dos-ricos-matam-os-pobres-de-virus-ou-de-fome. Acesso em: 01 set. 2022.

CRAVO, Daniela Copetti; JOELSONS, Marcela. A importância do CDC no tratamento de dados pessoais de consumidores no contexto de pandemia e de vacatio legis da LGPD. **Revista de Direito do Consumidor**, São Paulo, v. 131, ano 29, p. 111-145, set./out. 2020.

CRISTÓVAM, José Sérgio da Silva; HAHN, Tatiana Meinhart. Administração Pública orientada por dados: governo aberto e infraestrutura nacional de dados abertos. **Revista de Direito Administrativo e Gestão Pública**, Rio de Janeiro, v. 6, n. 1, p. 1-24, jan./jun. 2020.

DATA PRIVACY BRASIL. **Os dados e o vírus:** pandemia, proteção de dados e democracia. São Paulo: Reticências Creative Design Studio, 2020.

DATA PRIVACY BRASIL. Uma investigação sobre tecnologias baseadas em dados pessoais, usadas no combate à COVID-19 no Brasil. **Os dados virais**, 2021. Disponível em: https://osdadosvirais.dataprivacybr.org/. Acesso em: 04 set. 2022.

DECOLAR é multada em R$ 2,5 milhões por oferecer melhores preços a clientes que estão fora do Brasil. **Governo Federal**, 2022. Disponível em: https://www.gov.br/mj/pt-br/assuntos/noticias/decolar-e-multada-em-r-2-5-milhoes-por-oferecer-melhores-precos-a-clientes-que-estao-fora-do-brasil. Acesso em: 01 set. 2022.

DONEDA, Danilo. A proteção de dados em tempos de coronavírus: a LGPD será um elemento fundamental para a reestruturação que advirá após a crise. **Jota Info**, 2020. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/a-protecao-de-dados-em-tempos-de-coronavirus-25032020. Acesso em: 04 set. 2022.

DONEDA, Danilo Cesar Maganhoto. Considerações iniciais sobre os bancos de dados informatizados e o direito à privacidade. *In*: TEPEDINO, Gustavo (org.). **Problemas de direito civil-constitucional**. Rio de Janeiro: Renovar, 2000. p. 111-136.

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

DUARTE, Alan; NEGÓCIO, Ramon de Vasconcelos. Todos são iguais perante o algoritmo? Uma resposta cultural do direito à discriminação algorítmica. **Revista Direito Público**, Brasília, v. 18, n. 100, p. 218-244, out./dez. 2021.

EUROPA. Conselho Europeu. **Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data**. Europa: Conselho Europeu, 1981. Disponível em: https://rm.coe.int/1680078b37. Acesso em: 04 set. 2022.

FALEIROS JÚNIOR, José Luiz de Moura. **Administração Pública Digital**: proposições para o aperfeiçoamento do regime jurídico administrativo na sociedade da informação. Indaiatuba/SP: Editora Foco, 2020.

FALEIROS JÚNIOR, José Luiz de Moura. Dados anonimizados e o controle de aglomerações na pandemia da COVID-19. **Migalhas**, 2020. Disponível em: https://www.migalhas.com.br/coluna/migalhas-de-protecao-de-dados/338324/dados-anonimizados-e-o-controle-de-aglomeracoes-na-pandemia-da-covid-19. Acesso em: 04 set. 2022.

FALEIROS JÚNIOR, José Luiz de Moura; MARTINS, Guilherme Magalhães. Proteção de dados e anonimização: perspectivas à luz da Lei nº 13.709/2018. **Revista Estudos Institucionais**, Rio de Janeiro, v. 7, n. 1, p. 376-397, jan./abr. 2021.

FERREIRA, Keila Pacheco; RESENDE, Ana Paula Bougleux Andrade. Histórico normativo da proteção de dados pessoais no ordenamento jurídico brasileiro: avanços e retrocessos na tutela da privacidade. **Revista de Direito do Consumidor**, São Paulo, v. 137, ano 30, p. 85-112, set./out. 2021.

FRAZÃO, Ana. Decisões algorítmicas x Decisões humanas: as falhas das decisões humanas justificam a sua substituição pelas decisões algorítmicas? **Professora Ana Frazão**, 2022. Disponível em: http://professoraanafrazao.com.br/files/publicacoes/2022-04-06-Decisoes_algoritmicas_x_decisoes_humanas_As_falhas_das_decisoes_humanas_justificam_a_sua_substituicao_pelas_decisoes_algoritmicas.pdf. Acesso em: 30 ago. 2022.

FRAZÃO, Ana. Discriminação algorítmica: algumas conclusões. **Professora Ana Frazão**, 2021. Disponível em: http://professoraanafrazao.com.br/files/publicacoes/2021-09-29-Discriminacao_algoritmica_algumas_conclusoes_Existem_riscos_suficientes_a_exigir_maior_cuidado_e_transparencia_na_adocao_de_julgamentos_algoritmicos_Parte_XV.pdf. Acesso em: 01 set. 2022.

GABRIEL, Anderson de Paiva; DAVID, Ivana. Tecnologias de 'contact tracing' e a proteção dos dados de localização: quem é, contemporaneamente, o Leviatã de Hobbes? **Jota Info**, 2020. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/juiz-

hermes/tecnologias-de-contact-tracing-e-a-protecao-dos-dados-de-localizacao-22062020. Acesso em: 03 set. 2022.

GASIOLA, Gustavo Gil; MACHADO, Diego; MENDES, Laura Schertel. A Administração Pública entre a transparência e a proteção de dados. **Revista de Direito do Consumidor**, São Paulo, v. 135, ano 30, p. 179-201, maio/jun.2021.

GOVERNO brasileiro promove Seminário para debater proteção de dados do setor público. **LGPD News**, 2021. Disponível em: https://lgpdnews.com/2021/04/governo-brasileiro-promove-seminario-para-debater-protecao-de-dados-no-setor-publico/. Acesso em: 04 set. 2022.

GREEN, Ben; HU, Lily. The Myth in the Methodology: Towards a Recontextualization of Fairness in Machine Learning. **Harvard University**, 2018. Disponível em: https://scholar.harvard.edu/files/bgreen/files/18-icmldebates.pdf. Acesso em: 30 ago. 2022.

HARARI, Yuval Noah. **Homo Deus**: uma breve história do amanhã. São Paulo: Companhia das Letras, 2016.

HARARI, Yuval Noah. **Notas sobre a pandemia**: e breves lições para o mundo pós coronavírus. São Paulo: Companhia das Letras, 2020.

HARARI, Yuval Noah. The world after coronavirus. **Financial Times**. Disponível em: https://on.ft.com/2KD15M0. Acesso em: 01 set. 2022.

ISOLAMENTO é mais respeitado na periferia de São Paulo, diz estudo. **Notícias R7**, 2020. Disponível em: https://noticias.r7.com/sao-paulo/isolamento-e-mais-respeitado-na-periferia-de-sao-paulo-diz-estudo-29062022. Acesso em: 01 set. 2022.

ISSO não é peste negra; não é como se não tivéssemos ideia do que está matando as pessoas, diz Harari. **BBC News Brasil**, 2020. Disponível em: https://www.bbc.com/portuguese/internacional-52268811. Acesso em: 01 set. 2022.

JUNQUEIRA, Thiago. **Tratamento de Dados Pessoais e Discriminação Algorítmica nos Seguros**. São Paulo: Thomson Reuters Brasil, 2020.

KONDER, Carlos Nelson. O tratamento de dados sensíveis à luz da Lei. 13.709/2018. *In*: TEPEDINO, Gustavo; et al. **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro**. São Paulo: Thomson Reuters, 2019.

LAURA Schertel Mendes: Medida Provisória subverte conceito de liberdade na internet. **O Globo**, 2021. Disponível em: https://blogs.oglobo.globo.com/fumus-boni-iuris/post/laura-schertel-mendes-medida-provisoria-subverte-conceito-de-liberdade-na-internet.html. Acesso em: 04 set. 2022.

MACHADO, Diego Carvalho; MENDES, Laura Schertel. Tecnologia de perfilamento e dados agregados de geolocalização no combate à COVID-19 no Brasil: uma análise dos riscos individuais e coletivos à luz da LGPD. **Direitos Fundamentais & Justiça,** Belo Horizonte, ano 14, número especial, p. 105-148, nov. 2020.

MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. **LGPD**: Lei Geral de Proteção de Dados comentada. 2. ed. São Paulo: Thomson Reuters Brasil, 2019.

MANTELERO, Alessandro. From Group Privacy to Collective Privacy: Towards a New Dimension of Privacy and Data Protection in the Big Data Era. *In*: TAYLOR, Linnet; FLORIDI, Luciano; SLOOT, Bart van der (Ed.). **Group Privacy**: New Challenges of Data Technologies. Dordrecht: Springer, 2017. p. 139-158.

MARTINS, Marcelo Guerra; TATEOKI, Victor Augusto. Proteção de dados e democracia: fake news, manipulação do eleitor e o caso Cambridge Analytica. **Redes:** Revista Eletrônica Direito e Sociedade, Canoas, v. 7, n. 3, p. 135-148, out. 2019.

MEDIDA Provisória transforma a Autoridade Nacional de Proteção de Dados em autarquia. **Câmara dos Deputados**, 2022. Disponível em: https://www.camara.leg.br/noticias/886604-medida-provisoria-transforma-a-autoridade-nacional-de-protecao-de-dados-em-autarquia/. Acesso em: 04 set. 2022.

MELO, Maria Heloísa Chiaverini de; MIRANDA, João Irineu de Resende; TABORDA, Luiz Edemir; ROHMANN, Shana. Uma análise de conjuntura da Lei Geral de Proteção de Dados Pessoais (LGPD): tramitação, aprovação e vigência. **Revista Humanidades e Inovação**, Palmas, v. 8, n. 47, p. 55-70, junho 2021.

MENDES, Gilmar Ferreira; COELHO, Inocêncio Martires; BRANCO, Paulo Gustavo Gonet. **Curso de direito constitucional**. São Paulo: Saraiva, Instituto Brasiliense de Direito Público, 2007.

MENDES, Laura Schertel; DONEDA, Danilo. Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados. **Revista de Direito do Consumidor**, São Paulo, v. 120, ano 27, p. 469-483, nov./dez. 2018.

MENDES, Laura Schertel; MATTIUZZO, Marcela. Discriminação algorítmica: conceito, fundamento legal e tipologia. **Revista Direito Público**, Porto Alegre, v. 16, n. 90, p. 39-64, nov./dez. 2019.

MONTEIRO, Renato Leite. Lei Geral de Proteção de Dados do Brasil: análise contextual detalhada. **Jota Info**, 2018. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/lgpd-analise-detalhada-14072018. Acesso em: 04 set. 2022.

MP aciona Vivo, Tim, Oi e Claro por compartilhamento indevido de dados pessoais. **Ministério Público do Estado da Bahia**, 2022. Disponível em: https://www.mpba.mp.br/noticia/60732. Acesso em: 04 set. 2022.

NEGRI, Sergio Marcos Carvalho de Ávila; KORKMAZ, Maria Regina Detoni Cavalcanti Rigolon; FERNANDES, Elora Raad. Portabilidade e proteção de dados pessoais: tensões entre pessoa e mercado. **Civilistica.com**, Rio de Janeiro, v.10, n. 1, p. 1-39, maio 2021.

OLIVEIRA, Vinícius da Silva. **Lei Geral de Proteção de Dados Pessoais e Administração Pública: aplicação da norma**. 2021. Monografia (Graduação em Direito) – Faculdade de Direito, Universidade do Sul de Santa Catarina, Tubarão, 2021.

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT. Protecting Privacy in a Data-driven Economy: taking stock of current thinking. **Directorate for science, technology and industry – Committee on Digital Economy Policy**. maio 2014.

PACHECO alega inconstitucionalidade e devolve MP das fake news. **Senado Federal**, 2021. Disponível em: https://www12.senado.leg.br/radio/1/noticia/2021/09/14/pacheco-alega-inconstitucionalidade-e-devolve-mp-das-fake-news. Acesso em: 04 set. 2022.

PECK, Patrícia. **Proteção de dados pessoais**: comentários à Lei n. 13.709/2018 (LGPD). 3. ed. São Paulo: Saraiva, 2021.

PECK, Patrícia. 2020: o ano da privacidade e da proteção de dados nas Américas. **Febraban Tech**, 2020. Disponível em: https://noomis.febraban.org.br/especialista/patricia-peck-pinheiro/2020-o-ano-da-privacidade-e-protecao-de-dados-nas-americas. Acesso em: 04 set. 2022.

PREFEITURA do Recife usa tecnologia como aliada na contenção do novo coronavírus. **Prefeitura do Recife**, 2020. Disponível em: https://www2.recife.pe.gov.br/noticias/24/03/2020/prefeitura-do-recife-usa-tecnologia-como-aliada-na-contencao-do-novo-coronavirus. Acesso em: 04 set. 2022.

RODOTÀ, Stefano. **A vida na sociedade da vigilância: a privacidade hoje**. 1. ed. Rio de Janeiro: Renovar, 2008.

RODRIGUES, Yuri Gonçalves dos Santos; FERREIRA, Keila Pacheco. A privacidade no ambiente virtual: avanços e insuficiências da Lei Geral de Proteção de Dados no Brasil (Lei 13.709/18). **Revista de Direito do Consumidor**, São Paulo, v. 122, ano 28, p. 181-202, mar./abril. 2019.

SP contra o novo coronavírus: adesão ao isolamento social em SP. **Governo do Estado de São Paulo**, 2022. Disponível em: https://www.saopaulo.sp.gov.br/coronavirus/isolamento/. Acesso em: 04 set. 2022.

TENE, Omer. Privacy law's midlife crisis: a critical assessment of the second wave of global privacy laws. **Ohio State Journal**, Columbus, v. 74, n. 6, p. 127-1262, 2013.

UNIÃO EUROPEIA. **Carta dos Direitos Fundamentais da União Europeia**. **2000/C 364/01.** Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32000X1218(01)&from=EN. Acesso em: 04 set. 2022.

UNIÃO EUROPEIA. **Diretrizes 4/2020 sobre a utilização de dados de localização e meios de rastreio de contatos no contexto do surto de COVID-19**. Disponível em: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_pt.pdf. Acesso em: 03 set. 2022.

UNIÃO EUROPEIA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016.** Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=EN. Acesso em: 03 set. 2022.

VARÍOLA dos macacos não terá a mesma escala da COVID-19, afirma especialista. **CNN Brasil**, 2022. Disponível em: https://www.cnnbrasil.com.br/saude/variola-dos-macacos-nao-tera-a-mesma-escala-da-covid-19-afirma-especialista/. Acesso em: 01 set. 2022.

VEJA quais são os bairros do Recife com maior índice de isolamento social no combate ao coronavírus. **Uol**, 2020. Disponível em: https://jc.ne10.uol.com.br/pernambuco/2020/03/5603483-veja-quais-sao-os-bairros-do-recife-com-maior-indice-de-isolamento-social-no-combate-ao-coronavirus.html. Acesso em: 01 set. 2022.

VIEIRA, Gustavo Duarte. **Proteção de dados pessoais em práticas de profiling no setor privado**. 2019. Dissertação (Pós-Graduação em Direito) – Faculdade de Direito, Universidade Federal de Minas Gerais, Belo Horizonte, 2020.

VIOLA, Mario; TEFFÉ, Chiara Spadaccinni de. Tratamento de Dados Pessoais na LGPD: estudo sobre as bases legais dos artigos 7º e 11. *In*: BIONI, Bruno (org.). **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021. p. 117-148.

WACHTER, Sandra; MITTELSTADT, Brent. A right to reasoanable inferences: re-thinking data protection law in the age of big data and AI. **Columbia business law review**, New York, v. 2019, n. 2, p. 496-498, maio 2019.

WIMMER, Miriam. Proteção de dados em tempos de pandemia: novos paradigmas para o compartilhamento e o uso secundário de dados no poder público. **Panorama setorial da internet**, São Paulo, n. 4, ano 13, dez. 2021.

ZANATTA, Rafael A. F.; BIONI, Bruno R.; KELLER, Clara Iglesias; FAVARO, Iasmine L. Os dados e os vírus: tensões jurídicas em torno da adoção de tecnologias de combate à COVID-19. **Direitos Fundamentais & Justiça**, Belo Horizonte, ano 14, número especial, p. 231-256, nov. 2020.