DOI: https://doi.org/10.17921/2448-2129.2023v24n1p29-38

Monitoramento e Compartilhamento de Dados: a Suposta Antinomia entre o Poder de Vigilância Sanitária e a Lei Geral de Proteção de Dados

Monitoring and Data Sharing: the Alleged Antinomy Between the Power of Health Surveillance and the Data Protection Law

Marcos Antonio Madeira de Mattos Martins[a]; Luíza Pattero Foffano[a]; Alessandro Marco Rosini*[b]

[a]Pontifica Universidade Católica. SP, Brasil.
[b]Universidade Anhanguera de São Paulo. SP, Brasil.
*E-mail: alessandro.rossini@yahoo.com

Resumo

O presente artigo teve como objetivo o estudo de normas que autorizaram o compartilhamento de dados por empresas de telefonia com entidades governamentais, para fins de suporte à produção estatística oficial durante a situação de emergência de saúde pública decorrente do novo coronavírus. A pesquisa analisou as justificativas do Poder Público para coleta, compartilhamento e monitoramento de dados sem a devida autorização dos usuários ou mecanismos de proteção e segurança capazes de evitar e combater acessos não autorizados, vazamentos acidentais ou utilização indevida. Através de pesquisas doutrinárias e interpretações sobre a ciência jurídica, ficou afastada suposta antinomia entre normas relacionadas ao poder de vigilância sanitária e as garantias constitucionais do direito à liberdade e à autodeterminação da informação. A método utilizado nesse estudo foi realizada de forma exploratória, associada à pesquisa bibliográfica e legislativa, além de levantamentos de dados governamentais e informações disponíveis em redes públicas e privadas sobre o tema. O direito à privacidade e a garantia do sigilo de dados não podem ser violados pelo monitoramento e compartilhamento de dados, sem que haja plena segurança **técnica** e transparência na forma de sua utilização, pois a proteção dos direitos fundamentais deve ser priorizada em relação aos novos engenhos tecnológicos.

Palavras-chave: Direito à Privacidade. LGPD. Autodeterminação Informativa. Poder Público. Pandemia.

Abstract

This article aimed to study the rules that authorized the sharing of data by telephone companies with governmental entities, in order to support the official statistical production during the public health emergency situation resulting from the new coronavirus. The research analyzed the Government's justifications for collecting, sharing and monitoring data without the proper authorization of users or protection and security mechanisms capable of preventing and combating unauthorized access, accidental leaks or misuse. Through doctrinal research and interpretations of legal science, the supposed antinomy between norms related to the power of health surveillance and the constitutional guarantees of the right to freedom and self-determination of information was ruled out. The method used in this study was carried out in an exploratory way, associated with bibliographical and legislative research, in addition to surveys of government data and information available in public and private networks on the subject. The right to privacy and the guarantee of data secrecy cannot be violated by monitoring and sharing data, without full technical security and transparency in the way it is used, since the protection of fundamental rights must be prioritized in relation to new devices technological.

Keywords: *Right to Privacy. LGPD. Informative Self-Determination. Public Power. Pandemic.*

1 Introdução

A polêmica criada pelo rastreamento de pessoas para combate ao novo coronavírus coloca em debate o direito à privacidade das pessoas e a política de saúde pública. A Medida Provisória 954/2020 autorizou o compartilhamento de dados por empresas de telecomunicações prestadoras de Serviço Telefônico Fixo Comutado e de Serviço Móvel Pessoal com a Fundação Instituto Brasileiro de Geografia e Estatística, para fins de suporte à produção estatística oficial durante a situação de emergência de saúde pública de importância internacional decorrente do coronavírus (covid-19), de que trata a Lei nº 13.979, de 6 de fevereiro de 2020. A citada norma deixou de ter eficácia após decisão do plenário do Eg. Supremo Tribunal Federal, que referendou medida cautelar na Ação Direta de Inconstitucionalidade movida pelo Conselho Federal da Ordem dos Advogados do Brasil – CFOAB (ADI 6387 MC-REF/DF), prevalecendo a proteção das cláusulas constitucionais da liberdade individual e da privacidade. Apesar de a decisão ter sido proferida em maio de 2020, os órgãos públicos continuaram a utilizar das informações para controlar o isolamento social e as demais medidas de prevenção da proliferação do coronavírus.

A administração dos entes federativos defende a viabilidade jurídica de monitoramento dos dados pelo fato de que as informações pessoais compartilhadas por empresas de telefonia disponibilizam apenas a geolocalização da pessoa e que o anonimato dos usuários seria respeitado. Entretanto, subsistem dúvidas sobre os mecanismos de proteção de dados, e, ainda, há severos questionamentos sobre a ausência de proteção efetiva contra acessos não autorizados ou vazamentos

acidentais, que poderiam ter ocorrido durante o período.

Na mesma época em que ocorreu a publicação da MP 954/2020, a Lei Geral de Proteção de Dados (LGPD), publicada em 2018 e em vigor a partir de agosto de 2020 (após dois anos da sua edição), foi criada para possibilitar maior segurança no tratamento de dados pessoais, inclusive nos meios digitais, seja por pessoa natural, seja por pessoa jurídica de direito público e privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade dos indivíduos.

A citada lei de proteção de dados contempla, dentre outros fundamentos, o direito à privacidade e à autodeterminação informativa, fortalecendo a inviolabilidade da intimidade, da honra e da imagem. Com esse propósito, a LGPD destaca a necessidade de o usuário consentir expressamente sobre a possibilidade de o detentor dos dados repassar tais informações a terceiros e, ainda, a entidades públicas e privadas.

O embasamento nuclear da LGPD concentra-se na Constituição Federal, especificamente no artigo 5º, que trata dos direitos e garantias fundamentais, direitos e deveres individuais e coletivos, por onde está cravada a garantia de que são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito à indenização pelo dano material ou moral decorrente de sua violação (inc. X do art. 5º da Carta Federal).

Por seu turno, o Poder Público justifica a adoção de tais medidas com base na Constituição Federal, que prevê, dentre os direitos sociais proclamados, a saúde, a segurança, o trabalho, a moradia, a educação (art. 6º da Constituição Federal). A saúde pública é direito de todos e dever do Estado, devendo ser implementada mediante políticas sociais e econômicas que visem à redução do risco de doença e de outros agravos e ao acesso universal e igualitário às ações e serviços para sua promoção, proteção e recuperação.

O grande cerne deste debate é o fato de os usuários não terem a transparência necessária e a segurança das operadoras de telefonia sobre o conteúdo dos dados pessoais e sensíveis que elas possuem, e, ainda, não saberem quais medidas de proteção essas empresas utilizam para guardar as informações.

No presente trabalho, busca-se investigar a amplitude das garantias fundamentais do direito à privacidade e à autodeterminação da informação como forma de resistência à cessão de dados feita pelas concessionárias de telefonia aos governos, bem como esclarecimento dos mecanismos de controle de compartilhamento, para se apurar de que forma os dados cedidos estão sendo tratados com segurança e proteção, a fim de evitar o comprometimento da privacidade de dados pessoais e sensíveis de cada cidadão.

2 Desenvolvimento

2.1 Metodologia

A metodologia da pesquisa utilizada nesse estudo foi a exploratória, associada à pesquisa bibliográfica e legislativa, além de levantamentos de dados governamentais e informações disponíveis em redes públicas e privadas sobre o tema. Os referenciais teóricos utilizados constam em livros, teses, e artigos contidos em base de dados especializadas, como SciELO, entre outras.

2.2 Fundamentos do Direito à Privacidade e à Proteção dos Dados Pessoais

A proteção à privacidade, como um direito de personalidade, é inerente ao homem e tem por escopo a preservação dos atributos da dignidade da pessoa humana.

O direito à privacidade é visto por Tércio Sampaio Ferraz Jr. como "um direito subjetivo fundamental, cujo titular é toda pessoa física ou jurídica", tendo por objeto "a faculdade de constranger os outros ao respeito e de resistir à violação do que lhe é próprio (...); e cujo objeto é a integridade moral do titular" (FERRAZ, 1993, p. 77).

Na mesma linha, Celso Ribeiro Bastos assevera que o direito à privacidade consiste na faculdade do indivíduo de fazer cessar a intromissão de terceiros em sua vida privada, assim como de impedir-lhes o acesso a informações privadas e divulgação sobre esta área da manifestação existencial do ser humano (BASTOS, 1984).

A tutela à privacidade encontra previsão na Declaração dos Direitos do Homem e do Cidadão, de 1789, e na Declaração Universal dos Direitos do Homem, de 1948 (art. 12), e, ainda, está amparada pelo ordenamento jurídico pátrio, na Carta Magna, bem como no Código Civil e demais legislações.

Segundo os ditames do artigo 5º, inciso X, da Constituição Federal, "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação" (BRASIL, 1988).

O direito à privacidade também está consagrado no Código Civil, no capítulo dos direitos da personalidade, em seu artigo 21, consoante o qual "a vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma" (BRASIL, 2002).

É certo que, com o avanço tecnológico, surgiram novos delineamentos ao instituto da privacidade, em razão dos impactos causados à vida íntima do ser humano no âmbito da rede mundial de comunicação e informação.

Ante a formação de bancos de dados online e a dimensão de informações processadas mecanicamente, de forma instantânea, despontou a necessidade da proteção aos dados pessoais, tida como um complemento ao direito fundamental à privacidade, contextualizado para a era digital.

Nesse sentido, entende Doneda (2006, p.92):

> A proteção dos dados pessoais compreende, basicamente, pressupostos ontológicos idênticos aos da própria proteção da privacidade: pode-se dizer que é a sua "continuação por outros meios". Ao realizar esta continuidade, porém, assume a tarefa de conduzir uma série de interesses cuja magnitude

> aumenta consideravelmente na sociedade pós-industrial e acaba, por isso, assumindo uma série de características próprias – especialmente na forma de atuar os interesses que protege, mas também em referências a outros valores e direitos fundamentais.

A proteção de dados pessoais configura-se a partir da interpretação conjunta da Constituição Federal, do Código Civil, da Lei de Acesso à Informação (em especial da seção V intitulada "Das Informações Pessoais") e do Marco Civil da Internet (Lei 12.965/2014).

A Lei de Acesso à Informação (Lei n. 12.527/2011) dispõe, no artigo 31, que o tratamento de informações pessoais há de ser realizado de forma transparente, "com respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais" (BRASIL, 2011). Preconiza, ainda, a imprescindibilidade do consentimento expresso do titular para divulgação ou acesso por terceiros dos dados pessoais, no inciso II do parágrafo primeiro do mesmo dispositivo.

Soma-se a esse panorama normativo o Marco Civil da Internet (Lei n. 12.414/2011), em que está prevista, no artigo 7º, inciso I, a inviolabilidade da vida privada, bem como sua proteção e indenização pelo dano decorrente de sua violação, seja ele material, seja ele moral.

Mencionada lei federal dispõe, ainda, sobre o princípio do consentimento, enquanto elemento basilar da proteção de dados pessoais. No inciso IX do artigo 7º, o Marco Civil da Internet exige o "consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais" (BRASIL, 2014).

Ressalta-se, ainda, que o Marco Civil designa, no artigo 3º, incisos II e III, a proteção da privacidade e dos dados pessoais como princípio da disciplina do uso da internet no Brasil, frisando tal preceito nos artigos 7º, 8º e 10, inclusive.

Logo, a integração da sociedade em ambiente virtual tem fomentado um novo cenário para o direito à privacidade, uma vez estendida a vida privada à esfera dos dados pessoais em sua forma digital, fato este que tem sido assimilado pelo ordenamento jurídico pátrio.

2.3 Autodeterminação Informativa como Garantia Fundamental na Proteção de Dados Pessoais

A tutela dos dados pessoais emana de uma garantia constitucional revelada como direito à privacidade. É norma jurídica imperativa, pois "prescreve as condutas devidas e os comportamentos proibidos" relacionadas à essa previsão normativa (DINIZ, 1998).

Nessa ordem, a Diretiva Europeia de Proteção de Dados Pessoais (Diretiva 95/46/CE de 1995), em seu artigo 1º, preceitua seu objetivo:

Os Estados-membros assegurarão, em conformidade com a presente diretiva, a proteção das liberdades e dos direitos fundamentais das pessoas singulares, nomeadamente do direito à vida privada, no que diz respeito ao tratamento de dados pessoais. (EUROPA, 1988)

Vê-se, desse modo, que o direito europeu incorporou os dados pessoais ao âmbito da tutela à privacidade.

A Diretiva define, em seu artigo 2º, o conceito de dados pessoais:

> qualquer informação relativa a uma pessoa singular identificada ou identificável (pessoa em causa); é considerado identificável todo aquele que possa ser identificado, direta ou indiretamente, nomeadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, econômica, cultural ou social. (EUROPA, 1988).

No próprio artigo 2º, a Diretiva prevê o tratamento de dados, como sendo "qualquer operação ou conjunto de operações efetuadas sobre dados pessoais, com ou sem meios automatizados" exemplificando "a recolha, registro, organização, conservação, adaptação ou alteração, recuperação, consulta, utilização, comunicação por transmissão, difusão ou qualquer outra forma de colocação à disposição" (EUROPA, 1988).

O Regulamento 2016/679, de 27 de abril de 2016, revogou as disposições contidas na Diretiva, trazendo novas concepções à proteção de dados pessoais e incluindo princípios basilares, como a transparência e o consentimento expresso (EUROPA, 2016).

Destaca-se que a Carta dos Direitos Fundamentais da União Europeia, no artigo 8º, também trouxe algumas previsões relevantes sobre a proteção dos dados pessoais:

1. Todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito.
2. Esses dados devem ser objeto de um tratamento legal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respectiva retificação.
3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente (EUROPA, 2016).

No cenário jurídico brasileiro, o reconhecimento da proteção de dados como um direito fundamental deriva da consideração dos riscos que o tratamento automatizado traze à proteção da personalidade do indivíduo, em observância às garantias constitucionais de igualdade substancial, liberdade e dignidade da pessoa humana, além da tutela da intimidade e da vida privada (DONEDA, 2006, p.13).

A fim de reforçar a proteção aos dados pessoais, tramitou no Congresso Nacional brasileiro o projeto da Lei 13.709/18, sancionada em agosto de 2018: a Lei Geral de Proteção de Dados Pessoais (LGPD).

Segundo os incisos I e X do artigo 5º da referida norma, trata-se de dado pessoal a "informação relacionada a pessoa natural identificada ou identificável", e, de seu tratamento, "toda operação realizada com dados pessoais, como as que se

referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, (...)" (BRASIL, 2018).

A Lei Geral de Proteção de Dados Pessoais definiu em seu bojo, ainda, no inciso XII do mesmo artigo supracitado, o consentimento, como a "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada" (BRASIL, 2018).

Vislumbra-se, a partir da análise dos dispositivos da Lei, a consagração ao princípio da autodeterminação informativa e a importância do consentimento livre.

A autodeterminação informativa é, portanto, o direito que cada pessoa possui de exercer o controle de seus dados pessoais, com a faculdade de decidir e autorizar se determinada informação ou dado pode ser objeto de cessão, uso ou transferência a terceiros.

Por estar explicitamente consagrado na Carta da República (inciso X do art. 5º) o direito à privacidade e à intimidade das pessoas está tutelado juridicamente como direito personalíssimo, não possível de ser violado, salvo em casos específicos e com autorização judicial.

Nesse contexto, o artigo 7º da LGPD dispõe que o tratamento de dados pessoais somente poderá ser realizado mediante o fornecimento de consentimento pelo titular. Consentimento este que, nos moldes do artigo 8º, deve ser fornecido por escrito ou por outro meio que demonstre a vontade do usuário.

Conforme entendimento de Doneda (2006, p.372):

> O consentimento compreender um poder conferido à pessoa de modificar sua própria esfera jurídica, com base na expressão de sua vontade. Sua utilização como instrumento paradigmático para a tutela dos dados pessoais deve ser verificada a partir dos efeitos da sua concreta aplicação ao caso dos dados pessoais e seus efeitos.

Evidente, portanto, a existência de um robusto regime jurídico de tutela de dados, sendo possível identificar o princípio do consentimento como elemento basilar e a existência de um valor jurídico à proteção de dados pessoais.

Por consequência, a ponderação dessa garantia com demais valores jurídicos de mesma relevância pode vir a legitimar eventual embate de direitos.

Resta, dentro do contexto de inviolabilidade da privacidade, a reflexão sobre a possibilidade de acesso aos dados das pessoas para promoção da saúde coletiva em meio a pandemia do coronavírus, tido como fundamento para a utilização dos sistemas de monitoramento de dados de geolocalização, como reflexo do monitoramento do isolamento no estado emergencial atual para proteção à vida.

2.4 O Monitoramento de Dados no Cenário Internacional Durante a Pandemia

Na luta contra a pandemia do COVID-19, os governos ao redor do mundo estão desenvolvendo novas tecnologias de monitoramento, apostando, inclusive, na vigilância digital e no uso de inteligência artificial, o que tem trazido riscos à proteção dos dados pessoais e da privacidade dos cidadãos (KLEIN, 2020).

Na Ásia, é recorrente a troca de dados entre os provedores de serviços de internet e de telefonia com as autoridades governamentais. Na Coreia do Sul, os locais em que pessoas infectadas já estiveram ficam registrados em um aplicativo, de modo que, ao se aproximar de algum desses locais, o indivíduo recebe um sinal de alarme, desde que preencha uma série de perguntas e forneça informações sobre sua saúde (EL PAÍS, 2020).

Na Inglaterra, o governo está requisitando dados anônimos de localização de celulares, a fim de apurar se os cidadãos estão ou não seguindo as determinações de distanciamento social da quarentena. Nos Estados Unidos, o Presidente já se reuniu com os representantes das empresas Google, Facebook, Apple, Amazon e IBM, para viabilizar o acesso governamental aos dados de localização e, assim, criar um sistema de monitoramento (WASHINGTON POST, 2020).

Na Europa, alguns países já haviam firmado acordos individuais com os provedores de internet, para ter acesso aos dados de localização dos indivíduos, e, recentemente, a própria a Comissão Europeia requisitou tais dados aos provedores de telefonia, em busca de tentar interromper a evolução da disseminação do vírus no continente. O órgão europeu pretende tomar as cautelas necessárias para manter as informações em segurança, a partir do anonimato, por exemplo, a fim de impedir a identificação individual de cada usuário, e da exclusão dos dados após o término da pandemia. Ademais, a Autoridade Europeia para a Proteção de Dados realizará análises sobre as informações coletadas, enquanto a Organização Mundial da Saúde (OMS) ressalta que deverá haver respeito à privacidade e aos direitos humanos (TUDO CELULAR, 2020).

O Comitê Europeu de Proteção de Dados (CEPD), um organismo europeu independente que contribui para a aplicação de regras em matéria de proteção de dados na União Europeia, publicou recentemente algumas orientações aos países membros quanto à questão da utilização de dados de geolocalização, para o combate à pandemia do coronavírus. O Comitê ressaltou que as leis de proteção de dados não se aplicam a dados que tenham sido apropriadamente anonimizados, aconselhando os Estados europeus a limitarem o uso de dados de localização de maneira a não identificar os indivíduos. Somente quando impossível o uso de dados anonimizados, o CEPD sugere a adoção de medidas regulatórias, para garantir a proporcionalidade das políticas de vigilância social (EUROPEAN DATA PROTECTION BOARD, 2020).

O governo espanhol tomou a iniciativa de utilizar a ferramenta do Google para criar um aplicativo de GPS, e, desse modo, rastrear os movimentos das pessoas. O aplicativo

permite a visualização de mapas, com as áreas de maior risco de contágio, podendo recomendar ou não a quarentena a potenciais infectados, além de verificar se as medidas de isolamento estão sendo observadas adequadamente (UNISINOS, 2020).

Na Alemanha, alguns pesquisadores estão desenvolvendo um aplicativo de rastreamento similar àquele utilizado na Coreia do Sul. O Instituto Robert Kock, uma agência federal de prevenção sanitária, utilizou dados móveis de pessoas diagnosticadas com a doença para encontrar potenciais contatos e prever a propagação do vírus (UNISINOS, 2020).

Em Israel, cerca de 400 pessoas receberam uma notificação do Ministério da Saúde do país, com um alerta de que estavam próximos de alguém que testou positivo para o vírus. A mensagem foi enviada após a análise dos movimentos desses usuários, contendo os seguintes dizeres: "você deve imediatamente se isolar [por 14 dias] para proteger seus parentes e o público" (OLHAR DIGITAL, 2020).

Ante o cenário internacional de uso de dados pessoais para o enfrentamento à pandemia de COVID-19, o Brasil também tem dado início ao monitoramento dos cidadãos, a fim de controlar a expansão do vírus no território nacional.

No Brasil, a Medida Provisória 954/2020, cuja eficácia foi suspensa por decisão do liminar referendada pelo Plenário do Supremo Tribunal Federal (SUPREMO TRIBUNAL FEDERAL, 2020), autorizava o compartilhamento de dados por empresas de telecomunicações prestadoras do Serviço Telefônico Fixo Comutado - STFC e do Serviço Móvel Pessoal - SMP com a Fundação Instituto Brasileiro de Geografia e Estatística – IBGE durante a situação de emergência de saúde pública de importância internacional decorrente do novo coronavírus (covid-19).

A citada MP 954/2020 atribuía às mencionadas empresas o dever de disponibilizar à Fundação IBGE, em meio eletrônico, a relação dos nomes, dos números de telefone e dos endereços de seus consumidores, pessoas físicas ou jurídicas e, ainda, estabelecia que os dados compartilhados deveriam ser utilizados direta e exclusivamente pela Fundação IBGE para a produção estatística oficial, com o objetivo de realizar entrevistas em caráter não presencial no âmbito de pesquisas domiciliares.

2.5 As Diretrizes da Organização Mundial da Saúde para Promoção do Bem-Estar Coletivo

Irrompe, nesse cenário, a discussão sobre eventual violação ao direito à proteção dos dados pessoais em razão do acesso do Poder Público sobre informações dos cidadãos. A indagação pertinente sobre o assunto aborda possível quebra do direito à privacidade das pessoas e o uso de dados não autorizados para monitoramento da mobilidade urbana (WHO, 2020).

A questão que sobressai diante desse embate é a recomendação – mais que necessária, diante do quadro atual – da Organização Mundial da Saúde (OMS) sobre a gestão pública da saúde e a indispensabilidade de se efetivar meios de controle de prevenção da disseminação do novo coronavírus (WHO, 2020).

Nesse sentido, a OMS publicou a primeira Resposta Estratégica COVID-19 e Plano de Preparação (SPRP) em 3 de fevereiro de 2020. O SPRP definiu a estratégia contendo três objetivos para combater a propagação e limitar os danos causados pela doença. Em primeiro lugar, os países devem disponibilizar informações em tempo real sobre a evolução da epidemiologia e dos riscos. O acesso a medicamentos deve ser feito em tempo hábil, com ênfase a fornecimentos, medicamentos e equipamento essenciais. Em segundo lugar, também a nível internacional, o SPRP definiu as medidas necessárias para garantir a clareza e um processo global transparente para definir a investigação e a inovação prioridades, acelerar e aumentar a investigação e o desenvolvimento, e assegurar a disponibilidade equitativa dos candidatos a terapias, vacinas e diagnósticos. Estas iniciativas a nível global alimentam diretamente para o terceiro objetivo crucial: aumentar a preparação (WORLD HEALTH ORGANIZATION, 2020).

Segundo a Organização Mundial de Saúde, a pandemia COVID-19 afetou diferentes países em diferentes maneiras, mas em todo o mundo ocorreram três características definidoras: (a) velocidade e escala: a doença espalhou-se rapidamente, e a sua capacidade de dispersão tem potencial para superar até mesmo os sistemas de saúde mais resilientes; (b) gravidade: estima-se que 20% dos casos sejam graves ou críticos, com um risco aumentado de doença grave em grupos etários mais idosos e em pessoas com certas condições subjacentes; (c) perturbações sociais e económicas: choques para a saúde e sociais sistemas de cuidados e medidas tomadas para controlar a transmissão teve amplas e profundas consequências socioeconômicas (WHO, 2020).

Frisa-se que a velocidade da propagação da doença, como característica da pandemia, interfere na interrelação do público e do privado, uma vez que medidas de combate ao coronavírus também estão sendo tomadas para coleta de informações (SILVA, 2022).

O mesmo ponto de interferência de tempo é fator relevante da sociedade digital. A velocidade é o elemento crucial da sociedade da informação. A velocidade é o que "converte o fenômeno em algo revolucionário: muitas transformações em pouco tempo impedem que se leve a cabo uma evolução ordenada", ou seja, uma

> comunidade moderna e desenvolvida distingue-se, não obstante, recisamente por sua soberania sobre os fatos que a afetam, desse modo, a velocidade imprimi um ritmo de tomada de decisões bem próximo da improvisação, quando não da imprudência (CEBRIÁN, 1999, p.143).

Segundo o SindiTelebrasil (Sindicato Nacional das Empresas de Telefonia e de Serviço Móvel Celular e Pessoal), os dados relativos a quase 220 milhões de aparelhos celulares

serão repassados com um dia de atraso de modo aglomerado, estatístico e anonimizado, a partir da coleta de informações por quase cem mil antenas. O sistema deve ficar pronto em até duas semanas (ÉPOCA, 2020).

Convergindo com as orientações da OMS, o governo brasileiro promulgou a Lei 13.979 de 6 de fevereiro de 2020, dispondo sobre as medidas para enfretamento da emergência de saúde pública de importância internacional decorrente do coronavírus pelo surto de 2019 e, desde o início do ano, enfrenta a pandemia com medidas de isolamento e quarentena, bem como determinou a realização compulsória de exames médicos, testes laboratoriais, coleta de amostras clínicas, além de vacinação e outras medidas profiláticas (ainda em fase de testes) e tratamento médicos específicos (BRASIL, 2020).

Sob o argumento de buscar informações coletivas sobre o cumprimento de medidas de isolamento social, alguns estados brasileiros lançaram campanha de cadastramento de dados para verificação da mobilidade social (AGÊNCIA BRASIL, 2022).

Tais mecanismos e sistema de geolocalização, todavia, embora se apresentem como meio de análise da mobilidade social – isolamento imprescindível em razão do espraiamento da doença – não demonstraram real clareza e segurança com manipulação de dados de seus usuários (WIMMER, 2022).

Essa questão entre a necessidade de rastreamento da mobilidade urbana por meio de celulares e o direito à privacidade e intimidade deve ser analisada de maneira mais perfunctória, pois as informações transferidas pelas concessionárias telefônicas para o Poder Público podem conter dados sensíveis e não autorizados para uso (WIMMER, 2022).

2.6 A Suposta Antinomia entre o Poder de Vigilância Sanitária Estatal e a Lei Geral de Proteção de Dados

Em nome da velocidade de se obter informações sobre medidas protetivas contra o avanço da pandemia, o Poder Público pode cometer abusos na eleição de mecanismos invasivos informacionais relacionados à privacidade de dados (STF, 2020).

Tem-se como exemplo dessa urgência a abordagem feita pelo governo do estado de São Paulo: em nome do monitoramento de circulação de pessoas, para rastreamento dos celulares, o governo de São Paulo encaminhou a seguinte mensagem durante os meses de março a julho de 2020, através da concessionária de telefonia: "Código mensagem 40199: Gov de SP informa: houve aumento de casos de coronavírus em sua região. Reforce as medidas de higienização e fique em casa. Acesse http://bit.ly/spcorona."

De forma automática, após ler a mensagem e buscando maiores informações, o usuário acessa tal mensagem, e com um "click", sem qualquer aviso, o programa já se instala no celular, violando a boa-fé contratual (STF, 2020).

Note-se que na referida mensagem falta os esclarecimentos e as informações necessárias para o acesso. O medo e a curiosidade induzem o usuário a clicar no link, como se fosse um livre "consentimento". A mensagem mencionada, todavia, recebida no celular, não é clara e explicativa no sentido de que irá ser feito o rastreamento do usuário on line, ferindo, portanto, o direito à informação qualificada e específica que todo cidadão tem direito. Essa foi umas das justificativas jurídicas das Ações Diretas de Inconstitucionalidade n. 6387, 6388, 6389, 6390 e 6393 que foram movidas por entidades contra a Medida Provisória que autorizava o compartilhamento de dados dos usuários do serviço telefônico para o IBGE, com liminar proferida em Medida Cautelar na Ação Direta de Inconstitucionalidade pelo Supremo Tribunal Federal de Relatoria da Min. Rosa Weber, em 07 de maio de 2020 (STF, 2020).

Em 04 de junho de 2020, o primeiro conflito foi resolvido pelo Tribunal de Justiça do Estado de São Paulo. Por seu Órgão Especial, o tribunal reconheceu a legitimidade do Sistema de Monitoramento Inteligente (SIMI) utilizado pelo governo paulista, para monitoramento dos índices de isolamento social, que foi alvo de questionamentos por meio de mandados de segurança impetrados por cidadãos que sustentam a violação de seus dados pessoais feitos pela plataforma. O governo estadual, por meio de seu procurador, sustentou sua defesa de que o sistema vendo sendo feito "dentro dos limites constitucionais e infraconstitucionais, evitando a interrupção da utilização de ferramenta de grande importância para o combate à propagação do COVID-19" (SÃO PAULO, 2020).

A decisão do citado Órgão Especial abriu precedente favorável ao Estado, pois ainda subsistem ações populares, ações civis públicas e mandados de segurança que discutem a mesma questão judicial (GOVERNO DE SÃO PAULO, 2020).

O mesmo método foi utilizado pelo prefeito Nelson Marchezan Júnior, de Porto Alegre/RS, que assinou acordo de cooperação técnica com a Associação Brasileira de Recursos em Telecomunicações (ABR), envolvendo as quatro maiores operadoras de celular do Brasil (Claro, TIM, Oi e Vivo), para acesso a um sistema que possibilita o monitoramento do índice de isolamento social. Será contabilizado o deslocamento de 2,5 milhões de celulares (chips) ativos em Porto Alegre, segundo dados da Teleco Inteligência em Telecomunicações. Segundo o prefeito, "(...) analisamos o cenário da pandemia diariamente, e a ajuda da tecnologia é fundamental para monitorar com maior precisão os efeitos das medidas de isolamento".

A plataforma calcula quantos aparelhos entraram e quantos saíram da área de cobertura das antenas (ERBs) espalhadas pela cidade. A partir dessas informações, é possível ter um mapa da mobilidade urbana, confrontar com os indicadores de saúde e tomar decisões no combate ao novo coronavírus. A parceria não tem custos ao Município (PREFEITURA DE POÁ, 2020).

Por outro lado, há precedente do Supremo Tribunal Federal que veda o uso arbitrário de compartilhamento e

monitoramento de dados sob o argumento de que existe uma grave crise sanitária. Ou seja, a Suprema Corte brasileira não admite a violação ao direito fundamental à autodeterminação informativa.

O Supremo Tribunal Federal, todavia, tem outro entendimento sobre o assunto. Através de decisão proferida na Ação Direta de Inconstitucionalidade (ADI 6387/2020), movida pelo Conselho Federal da Ordem dos Advogados do Brasil – CFOAB, com admissão de *amici curiae* da Associação Data Privacy Brasil de Pesquisa, do Laboratório de Políticas Públicas e Internet – LAPIN e do Instituto Brasileiro de Geografia e Estatística – IBGE, a douta Ministra Relatora Rosa Weber suspendeu a eficácia da Medida Provisória 954/2020, determinando que o IBGE se abstenha de requerer a disponibilização, pelas operadoras de telefonia, em meio eletrônico, dos dados de que trata e que dizem com os nomes, números de telefone e endereços de todos os seus usuários, pessoas físicas e jurídicas (SUPREMO TRIBUNAL FEDERAL, 2020).

A ADI 6387 contemplou a análise conjunta de outras ADIs: 6388, 6389, 6390 e 6393, ajuizadas por quatro partidos políticos: PSDB, PSB, PSOL e PCdoB, que também reiteravam a arguição de inconstitucionalidade formal e material da MP 954 de 17 de abril de 2020, todos distribuídos para Ministra Rosa Weber.

Embora subsista a decisão do STF, com determinação de proibição de compartilhamento e monitoramento de dados, diversas cidades e estados continuam utilizando o sistema inteligente de monitoramento de dados.

Algumas ponderações, portanto, devem ser destacadas para maior reflexão nesse contexto judicial, pois as medidas públicas de compartilhamento de dados destoam com a Lei Geral de Proteção de Dados e com a própria Constituição Federal.

O primeiro choque de interpretação aparenta elevar dois princípios ou garantias constitucionais previstas no ordenamento: o primeiro, resultante da necessidade de se efetivar meios de controle da pandemia (saúde pública) e, o segundo, que se refere ao direito à privacidade e à autodeterminação da informação (direito personalíssimo).

Gustavo Tepedino adverte que o cruzamento e a circulação de dados, especialmente aos dados sensíveis, podem ser obtidos facilmente com o "barateamento da tecnologia da informação". E, em razão dessa facilidade de aceso, Tepedino assevera que "há que se definir quando, onde, como e para que fins podem ser colhidas informações pessoais, impedindo-se seu tratamento como ativo comercial ou expressão do poder político do Estado" (TEPEDINO, 2014, p. 88).

Nesse patamar de valores jurídicos, não se verifica, nas medidas tomados pelo Poder Público, transparência ao respeito ao princípio da privacidade e intimidade, diante da falta de informação adequada e completa pela qual ocorreram e ocorrem a transmissão de dados aos usuários. A Lei Geral de Proteção de Dados (LGPD) abrange, dentre outros fundamentos, o direito à privacidade e a autodeterminação informativa, fortalecendo a inviolabilidade da intimidade, da honra e da imagem. Com esse propósito, a LGPD destaca a necessidade de o usuário consentir expressamente sobre a possibilidade de o detentor dos dados repassar tais informações a terceiros, e, ainda, a entidades públicas e privados (LEI 13.709/2018).

O embasamento nuclear da LGPD concentra-se na Constituição Federal, especificamente no artigo 5º, que trata dos direitos e garantias fundamentais, dos direitos e deveres individuais e coletivo, por onde está cravada a garantia de que são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação (inc. X, do art. 5º, da Carta Federal) (BRASIL, 1988). A mesma Carta Constitucional preconiza que é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal (BRASIL, 1988).

Não se pode admitir que medidas de preservação da saúde pública possam suprimir direitos personalíssimos de cada cidadão. Se o Órgão Especial do Tribunal de Justiça de São Paulo não observou os fundamentos e orientações do Supremo Tribunal Federal na ADI 6387/DF, a resposta lógica está vinculada à liberdade daquele tribunal de responder sobre o conflito que lhe fora provocado, por total autonomia de sua jurisdição. Entretanto, essa resposta jurisdicional específica não pode gerar a continuidade ou a reedição de medidas de monitoramento e compartilhamento de dados sem respeito às diretrizes da LGPD.

Por outro lado, o Tribunal de Justiça do Distrito Federal e dos Territórios (TJDFT), preocupado com a privacidade de dados das pessoas físicas, disponibilizou, no dia 08/09/2020, Resolução 9/2020, criando Política de Privacidade dos Dados das Pessoas Físicas – PPD. O ato normativo do TJDFT, embora não estar vinculado com o monitoramento do Poder Público, importa o integral cumprimento da Lei Geral de Proteção de Dados como fundamento para evitar danos ou prejuízos aos cidadãos que litigam naquele Tribunal (TRIBUNAL DE JUSTIÇA DO DISTRITO FEDERAL E DOS TERRITÓRIOS, 2020).

Não há, portanto, antinomia jurídica, vale dizer, inexiste um conflito aparente entre a Lei 13.979/2020, que dispõe sobre medidas para enfrentamento da emergência de saúde pública de importância internacional decorrente do coronavírus, e a Lei 13.709/2018, que reiterou o direito à privacidade ao conferir força à autodeterminação da informação, por meio da Lei Geral de Proteção de Dados (LGPD), pois é fato que nenhuma autoridade ou entidade pública e privada pode obter dados dos cidadãos através de sistema que não apresente mecanismos de proteção compatíveis com as cláusulas constitucionais de liberdade individual, da privacidade e do

livre desenvolvimento da personalidade, conforme dispõe o artigo 5º, "caput" e seus incisos X e XX, da Carta Federal (CARTA FEDERAL, 2020).

O direito à privacidade e à autodeterminação informacional não obsta o Poder Público de encontrar meios seguros e efetivos para manutenção da saúde pública. Não obstante, as situações de crise da saúde pública, como verificada na pandemia do novo coronavírus, não podem justificar o enfraquecimento das garantias constitucionais, contemplando supremacias e medidas excepcionais que contenham políticas de vigilância, mas que, ao mesmo tempo, violam o direito e a liberdade individual de cada cidadão (STF, 2022).

Bastos e Martins (1989, p. 63) entende que direito à privacidade é a:

> (...) faculdade que tem cada indivíduo de obstar a intromissão de estranhos em sua vida privada e familiar, assim como de impedir-lhes o acesso a informações sobre a privacidade de cada um, e também impedir que sejam divulgadas informações sobre esta área de manifestação existencial do ser humano.

A privacidade é direito fundamental e possui uma dimensão subjetiva por meio da qual o cidadão pode exigir de terceiros – particulares ou Estado – certos comportamentos negativos ou positivos em razão desse valor. E, ainda, possui dimensão objetiva, que se manifesta pelo ordenamento jurídico, como diretriz axiológica e limitador ao poder impositivo do Poder Público (STF, 2022).

A proteção desse valor fundamental do direito à privacidade deve sobrepor às eventuais medidas que o Estado imponha sobre as liberdades individuais de cada pessoa. No momento em que ocorre o uso de dados não autorizados pelo indivíduo em sistemas que possibilitam o acesso de terceiros, há violação do direito à privacidade.

3 Conclusão

Com a justificativa de prevenir a propagação do coronavírus em decorrência da pandemia de COVID-19 enfrentada atualmente no mundo, o governo federal, por meio de seu presidente, adotou a Medida Provisória 954 de abril de 2020, determinando o compartilhamento de dados por empresas de telecomunicações prestadoras de Serviços Telefônico Fixo Comutado e de Serviço Móvel Pessoal. Essa MP teve sua eficácia suspensa pelo STF, através da ADI 6387/DF e, consequentemente, deixou de ter força jurídica no território nacional.

Mesmo com a decisão do Supremo Tribunal Federal, subsistem governos estadual e municipal que ainda adotam medidas e sistemas inteligentes de monitoramento e compartilhamento de dados sem autorização de seus usuários, em total desrespeito ao direito à privacidade e à autodeterminação da informação.

Se o Poder Público justifica sua intervenção por meio de coleta e compartilhamento de dados, sob o argumento de que o bem maior que está sendo tutelado é a saúde pública, essa medida não pode não suprimir a privacidade e o sigilo de dados. A quebra do sigilo ou dado pessoal sem autorização expressa de cada indivíduo, somente pode ser feita em casos excepcionais e com autorização judicial específica, respeitando-se a razoabilidade e proporcionalidade da medida.

Além da impropriedade legislativa que justificou a edição da Medida Provisória 954/2020, ainda pode-se testificar que não houve atenção regulamentar na proteção dos dados pessoais de acessos não autorizados, ou, ainda, medidas contra vazamento acidentais ou utilização indevida. Mecanismos de devassa de informações e coleta de dados pessoais – como ocorreu na edição da citada MP – demonstram que não se pode confundir relevância e urgência de questões de ordem pública com atropelo de compartilhamento ilegal e irregular de dados pessoais.

A excepcionalidade da pandemia e a consequente medida emergencial para conter a propagação do coronavírus não pode justificar a criação de normas que violem os direitos fundamentais dos usuários dos serviços de telefonia. A forma de obtenção, compartilhamento (cessão) de dados e consequente monitoramento, deve prescindir de autorização expressa do usuário. Além disso, deve ser transparente e seguir protocolos de segurança para validação de quais dados são transmitidos, não podem gerar dúvidas sobre sua utilidade.

No mesmo sentido, o usuário deve obter informações claras, qualificadas e específicas no que diz respeito ao sistema de geolocalização dos usuários, sob pena de violar a liberdade individual de cada cidadão.

Não se trata, dentro do contexto normativo, de decidir sobre preponderância de políticas públicas sobre garantias individuais por força da saúde pública. Nesse caso, ambos princípios podem caminhar de forma harmônica, desde que sejam feitos protocolos efetivos para proteção de dados, em razão da boa-fé objetiva e princípios da finalidade, adequação e transparência das relações entre o Poder Público e os particulares.

De todo o modo, o enfrentamento da crise da saúde pública e a necessidade de obtenção de dados pessoais de cada usuário dos serviços de telefonia podem ser objeto de ajustes normativos, desde que respeitados os direitos fundamentais à liberdade e ao livre desenvolvimento da personalidade, com transparência de protocolos, limites temporais, observando-se os princípios da finalidade, da adequação, da transparência, da prevenção e da segurança das informações.

Referências

AGENCIA BRASIL. 2022. Disponível em https://agenciabrasil.ebc.com.br/geral/noticia/2020-04/covid-19-iniciativas-usam-monitoramento-e-geram-preocupacoes.

BASTOS, C.R. *Curso de direito constitucional*. São Paulo: Saraiva, 1984.

BASTOS, C.R.; MARTINS, I.G. *Comentários à Constituição do Brasil.* São Paulo: Saraiva, 1989.

BRASIL. *Constituição da República Federativa do Brasil de*

1988. Diário Oficial da União, Brasília, DF, 5 de outubro de 1988.

BRASIL. *Lei n. 10.406/2002*. Institui o Código Civil. Diário Oficial da União, Brasília, DF, 11 jan. 2002.

BRASIL. *Lei n. 12.527/2011*. 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. Diário Oficial da União, Brasília, DF, 18 nov. 2011. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 24 ago. 2022.

BRASIL. *Lei n. 12.965/2014*. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Diário Oficial da União, Brasília, DF, 23 abr. 2014. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 24 ago. 2022.

BRASIL. *Lei n. 13.709/2018*. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União, Brasília, DF, 14 ago. 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 14 set. 2022.

BRASIL. *Lei n. 13.979/2020*. Dispõe sobre as medidas para enfrentamento da emergência de saúde pública de importância internacional decorrente do coronavírus responsável pelo surto de 2019. Diário Oficial da União, Brasília, DF, 6 fev. 2020. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2020/Lei/L13979.htm>. Acesso em 19 out. 2022.

CARTA FEDERAL. Conforme artigo 5º, "caput" e seus incisos X e XX, da Carta Federal. Disponível em https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 19 out 2022.

CEBRIÁN, J.L. *A rede.* São Paulo: Summus, 1999.

DUDH - *Declaração Universal dos Direitos Humanos*, 1948. Disponível em: <http://www.dhnet.org.br/direitos/deconu/textos/integra.htm>.

DONEDA, D. *A Proteção dos Dados Pessoais como um Direito Fundamental.* Joaçaba, v.12, n.2, p.91-108, 2011.

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

DINIZ, M.H. *Compêndio de introdução à ciência do direito*. São Paulo: Saraiva, 1998.

EL PAÍS. *Coreia do Sul: contra o coronavírus, tecnologia*. Disponível em: <https://brasil.elpais.com/internacional/2020-03-15/coreia-do-sul-contra-o-coronavirus-tecnologia.html>. Acesso em: 24 ago. 2022.

ÉPOCA NEGÓCIOS. *Coronavírus: governo vai monitorar celulares para combater pandemia.* Disponível em: <https://epocanegocios.globo.com/Tecnologia/noticia/2020/04/coronavirus-governo-brasileiro-vai-monitorar-celulares-para-conter-pandemia.html>. Acesso em: 16 out. 2022.

EUROPA. *Carta dos direitos fundamentais da União Europeia*. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:12016P/TXT&from=FR>. Acesso em: 25 ago. 2022.

EUROPA. *DIRECTIVA 95/46/CE, de 24 de outubro de 1998*. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/LSU/?uri=CELEX:31995L0046>. Acesso em: 24 ago. 2022.

EUROPA. *RGPD, de 27 de abril de 2016.* Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=LEGISSUM%3A310401_2>. Acesso em: 24 ago. 2022.

EUROPEAN DATA PROTECTION BOARD. *Statement on the processing of personal data in the context of the COVID-19 outbreak*. Disponível em: <https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_2020_processingpersonaldataandcovid-19_en.pdf>. Acesso em: 24 ago. 2022.

GOVERNO DE SÃO PAULO. *TJ reconhece legalidade do Sistema de Monitoramento Inteligente do Governo de SP*. Disponível em: <https://www.saopaulo.sp.gov.br/noticias-coronavirus/tj-reconhece-legalidade-do-sistema-de-monitoramento-inteligente-do-governo-de-sp/>. Acesso em: 19 out. 2022.

INSTITUTO HUMANITAS UNISINOS. *Coronavírus, os governos europeus pedem socorro às Big Tech. Mas o tempo dos mapas de contágio está se esgotando.* Disponível em: <http://www.ihu.unisinos.br/78-noticias/597285-coronavirus-os-governos-europeus-pedem-socorro-as-big-tech-mas-o-tempo-dos-mapas-de-contagio-esta-se-esgotando>. Acesso em: 24 ago. 2022.

KLEIN, Naomi. Nesse sentido, sob o pretexto de preservar vidas na pandemia de coronavírus, governador de Nova York pede que bilionários invistam em tecnologia da vigilância. Disponível em https://www.intercept.com.br/2020/05/13/coronavirus-governador-nova-york-bilionarios-vigilancia/ - Acesso em: 20 maio 2022.

OLHAR DIGITAL. *Para combater o coronavírus, governos querem dados de localização.* Disponível em: <https://olhardigital.com.br/coronavirus/noticia/para-combater-o-coronavirus-governos-querem-dados-de-localizacao/98356>. Acesso em: 24 ago. 2022.

PREFEITURA DE POÁ. *Prefeitura usa dados de operadoras de celular para monitorar isolamento social.* Disponível em: <https://prefeitura.poa.br/gp/noticias/prefeitura-usa-dados-de-operadoras-de-celular-para-monitorar isolamento-social>. Acesso em: 19 out. 2022.

REINALDO FILHO, D. *A utilização de dados de geolocalização no combate à epidemia do coronavírus.* Juristas, 2020. Disponível em: <https://juristas.com.br/2020/03/29/a-utilizacao-de-dados-de-geolocalizacao-no-combate-a-epidemia-do-coronavirus/>. Acesso em: 3 set. 2022.

SAMPAIO FERRAZ, Tercio. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. *Cadernos de Direito Constitucional e Ciência Política*, n. 1. Disponível em file:///C:/Users/Windows/Downloads/67231-Texto%20do%20artigo-88644-1-10-20131125.pdf. Acesso em: 19 out. 2022.

SILVA, M.L.F.; TEIXEIRA, M.A.C.; FRANCISCO, E.R. *O Uso de dados pessoais no combate à COVID-19: alcances e limites das experiências do Brasil e da União Europeia*. Rev Gestão Países de Língua Port., Disponível em: https://bibliotecadigital.fgv.br/ojs/index.php/rgplp/article/view/85223/81660. Acesso em: 19 set. 2022.

STF. *Medida Cautelar na Ação Direta de Inconstitucionalidade 6.387 Distrito Federal*. Relatora: Min. Rosa Weber. DJ: 06/5/2020. Disponível em: <http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADI6387MC.pdf>. Acesso em: 19 nov. 2020.

TEPEDINO, Gustavo. Liberdades, tecnologia e teoria da interpretação. *Rev. Forense*, v.49, p.88, 2014.

TRIBUNAL DE JUSTIÇA DO DISTRITO FEDERAL E DOS TERRITÓRIOS. *TJDFT se antecipa à LGPD e cria Política de Privacidade dos Dados das Pessoas Físicas.* Disponível em: <https://www.tjdft.jus.br/institucional/imprensa/noticias/2020/setembro/tjdft-cria-politica-de-privacidade-dos-dados-das-

pessoas-fisicas-e-se-adequa-a-legislacao-federal>. Acesso em: 19 out. 2020.

TUDO CELULAR. *Coronavírus: operadoras passam a rastrear localização de celulares na Europa.* Disponível em: https://www.tudocelular.com/seguranca/noticias/n154217/operadoras-rastreiam-localizacao-celulares-europa.html. Acesso em 24 ago. 2020.

WASHINGTON POST. *U.S. government, tech industry discussing ways to use smartphone location data to combat coronavirus.* Disponível em: <https://www.washingtonpost.com/technology/2020/03/17/white-house-location-data-coronavirus/>. Acesso em: 24 ago. 2022.

WIMMER, M. *Limites e possibilidades para o uso secundário de dados pessoais no poder público.* Rev Bras. Pol. Públicas. UniCEUB. p.123. Disponível em file:///C:/Users/Windows/Downloads/7136-29768-1-PB.pdf. Acesso em: 19 jul. 2022.

WHO - World Health Organization. *COVID-19 Preparedness and Response Progress Report*. Disponível em: <file:///C:/Users/Windows/Downloads/srp-covid-19-6month.pdf> in <https://www.who.int/publications/m/item/who-covid-19-preparedness-and-response-progress-report---1-february-to-30-june-2020>. Acesso em: 19 out. 2020.