REVISTA DE DIREITO DA SAÚDE COMPARADO

Recebido em: 14/11/2022 Aceito em: 19/12/2022

DOI: https://doi.org/10.56242/direitodasaudecomparado;2022;1;1;189-205

Digital tracking and tracing (DTT) systems e o compartilhamento de dados pessoais no Brasil: estratégias de rastreamento de contágio do Covid-19 e o direito à privacidade[1]

Rubens Beçak

Professor Associado da Universidade de São Paulo (USP)
Professor no Programa de Pós-graduação da UNESP – Franca
Professor visitante da Universidad de Salamanca (USAL)

Guilherme de Siqueira Castro

Mestre em Direito pela Faculdade de Direito de Ribeirão Preto da Universidade de São Paulo – FDRP / USP.

Sumário

Introdução

O presente trabalho analisa a experiência brasileira de rastreamento e monitoramento digital de indivíduos, tecnologia conhecida em inglês como *Digital Tracking and Tracing (DTT) Systems*, no contexto da pandemia do Covid-19.

Em linhas gerais, essas tecnologias utilizam aplicativos de *smartphone* para registrar contato entre pessoas automaticamente, via *Bluetooth*, com o objetivo de informar eventual contato entre pessoas saudáveis e infectados pelo Covid -19, de tal sorte a

[1] Este texto foi publicado em versão original no livro "Discussões Sobre Direito na Era Digital", Anna Carolina Pinho (Coord.), Rio de Janeiro: GZ, 2021. Versão revista e totalmente atualizada.

encaminhar o usuário exposto ao contágio da doença ao isolamento social.

As tecnologias analisadas neste texto não são novas, já são empregadas para fins de inteligência e segurança nacional, no contexto da chamada luta global ao terrorismo. Inclusive, há notícia na imprensa internacional que Israel (ELSTRIN, 2021) e Paquistão (HASHIM, 2020), países onde o tema do terrorismo mobiliza o debate público, utilizaram seus sistemas digitais de rastreamento, operados por suas agências de inteligência e orginalmente criados para fins de contraterrorismo, para uso na emergência de saúde pública decorrente do novo coronavírus.

Comercialmente, as *Big Techs* como *Amazon*, *Facebook*, *Microsoft*, *Google* e *Apple*, também praticam o monitoramento dos usuários dos seus aplicativos, colecionando uma gama de dados comportamentais que são utilizados para financiar suas operações e obter lucro com publicidade digital e a prestação de serviços "personalizados" para os consumidores, fenômeno denominado como capitalismo de vigilância (ZUBOFF, 2019, p. 54).

Atualmente, em razão da emergência sanitária do Covid-19, os sistemas *DTT* passaram a ser aproveitados para auxiliar no controle epidemiológico da doença. O uso de sistemas de monitoramento e rastreamento digital para controlar o avanço da epidemia do Covid-19 foi acompanhado de uma crescente preocupação sobre privacidade ao redor do globo.

No Brasil, a polêmica chegou ao Supremo Tribunal Federal – STF, com o ajuizamento da Ação Direta de Inconstitucionalidade (ADI) nº 6.387, de autoria do Conselho Federal da Ordem dos Advogados do Brasil – CFOAB, contra a medida provisória nº 954/2020, que questionou o compartilhamento de dados pessoais dos usuários do serviço telefônico fixo comutado e do serviço móvel pessoal, pelas empresas de telecomunicações com o Instituto Brasileiro de Geografia e Estatística – IBGE (BRASIL, 2020). Além do precedente judicial, há a Lei da Quarentena com dispositivos semelhantes de compartilhamento de dados pessoais para fins de enfrentamento do Covid-19.

O presente texto objetiva problematizar todo esse arcabouço jurídico-regulatório à luz dos direitos fundamentais e dos princípios insculpidos na Lei Geral de Proteção de Dados – LGPD.

1. Privacidade: do direito de estar só ao direito da autodeterminação informativa

O direito à privacidade nasce com as revoluções liberais burguesas do final do século XVIII. A construção jurídica do direito à privacidade está baseada, historicamente, no direito à propriedade, pauta-chave das revoluções liberais. Dito de outra maneira, há uma relação de causalidade entre proteção da propriedade privada e a proteção da privacidade.

No liberalismo clássico, a privacidade seria uma esfera exclusiva do indivíduo burguês, inacessível a terceiros ou ao Estado sem consentimento do indivíduo. Cada indivíduo seria proprietário de sua esfera de intimidade. Nesta linha, a construção jurisprudencial do direito à privacidade em países da *common law* baseou-se em institutos jurídicos de proteção da propriedade privada, como *trespass*, *nuisance* e *conspiracy* (DONEDA, 2019, p. 109).

John Stuart Mill, no ensaio *'Sobre a liberdade'*, de 1859, concebeu um ambiente individual livre da ingerência da sociedade e do Estado, uma parte da vida pessoal, dos hábitos e do comportamento que interessa somente ao indivíduo e mais ninguém (MILL, 2003, p. 82). Mill não fala expressamente em direito à privacidade, mas estabelece as bases para o debate.

Em 1879, no *Treatise on Law of Torts*, Thomas Cooley, jurista americano, cunhou a expressão "direito de estar sozinho", sem relacioná-la com a noção de privacidade, mas com a de responsabilidade civil (COOLEY, 1879, p. 29). Em 1890, Louis Brandeis e Samuel Warren publicaram na *Harvard Law Review* o ensaio *'The Right to Privacy'*. No artigo, os autores utilizaram m a expressão "direito de estar sozinho" formulada por Cooley no contexto do direito à privacidade.

Preocupados com as inovações tecnológicas da época que possibilitavam a violação da intimidade de indivíduos, como a fotografia, bem como com a imprensa especializada em fofocas, os autores vão construir o conceito de direito à privacidade a partir de precedentes da *common law* que reconheceram proteção aos direitos individuais de personalidade (BRADEIS; WARREN, 1890, p. 205).

O impacto do ensaio de Bradeis e Warren foi significativo na academia estadunidense e na jurisprudência. A despeito do fato da Constituição americana não mencionar explicitamente o direito à privacidade, a Suprema Corte dos EUA reconheceu, em vários julgados ao longo do século XX, o status constitucional do direito à privacidade ou a garantias a certas zonas de privacidade (VIEIRA, 2002, p.86)

Fora dos EUA a recepção do direito à privacidade como um direito extrapatrimonial, vinculado à personalidade demorou. Somente após a Segunda Guerra Mundial, com a positivação do princípio da dignidade humana em várias constituições do pós-guerra e a revisão da separação absoluta entre Ética-Moral e o Direito (BEÇAK, 2011, p. 19), o direito à privacidade mereceu proteção jurídica.

Houve uma guinada nos sistemas de *civil law*, que passaram a conceber o direito à privacidade como o direito ao livre desenvolvimento da personalidade sem a interferência do controle estatal ou reprovação social. Neste sentido, o artigo 12 da Declaração Universal dos Direitos Humanos de 1948 estatui que "ninguém será sujeito à interferência em sua vida privada, em sua família, em seu lar ou em sua correspondência, nem a ataque à sua honra e reputação".

Na mesma linha, o artigo 17 do Pacto Internacional de Direitos Civis e Políticos de 1966 prescreve que "ninguém será sujeito a ingerências arbitrárias ou ilegais em sua vida privada, em sua família, em seu domicílio ou em sua correspondência, nem de ofensas ilegais às suas honra e reputação".

No Brasil, a Constituição Federal de 1988 é a primeira a prever, expressamente, na nossa história constitucional, a proteção ao direito à privacidade, no artigo 5º, inciso X: "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".

Além da previsão expressa ao direito à privacidade, a privacidade é reconhecida como direito fundamental em variadas expressões: privacidade e inviolabilidade do domicílio (artigo 5º, inciso XI), privacidade e sigilo das comunicações (artigo 5º,

inciso XII). O direito à privacidade também protege o indivíduo contra a devassa de suas movimentações bancárias (sigilo bancário) e de sua relação, como contribuinte, com o fisco (sigilo fiscal). Por fim, o direito à privacidade impõe um dever a certos profissionais, tais como médicos, advogados e jornalistas, de manter sigilo sobre informações que obtiveram conhecimento em virtude do exercício da profissão.

Oportuno consignar, ainda, que a doutrina brasileira trata o direito à intimidade e à vida privada como facetas do direito à privacidade. Todavia, há quem distinga os conceitos de intimidade e vida privada. Nesta linha, a intimidade representaria uma esfera mais restrita, um campo exclusivo que alguém reserva para si próprio, a salvo de qualquer intromissão estatal ou social, um direito ao isolamento, direito de não ser vigiado, enquanto a vida privada corresponderia a uma esfera mais ampla, que abrangeria também as relações pessoais mantidas pelo titular do direito, de não ter a vida íntima e familiar devassada, de não ter detalhes pessoais divulgados, nem de ter a imagem e o nome expostos contra a sua vontade (TAVARES, 2019, p. 550-551).

No que tange ao tema deste trabalho, os conceitos são insuficientes para dar conta de toda a complexidade que envolve o direito à privacidade na sociedade da informação, posto que a privacidade deve abranger também o direito do cidadão de exercer controle sobre o uso, a circulação e o armazenamento dos seus próprios dados pessoais.

Antigamente, havia entendimento doutrinário e jurisprudencial[2] que pugnava que a proteção constitucional prevista no artigo 5º, inciso XII, é da comunicação de dados e não dos dados em si. Para esta posição, tão-somente a comunicação privativa é que não pode ser violada por sujeito estranho à comunicação, sob pena de imunizar a produção de dados ilegais ou incriminadores relativos a uma pessoa (FERRAZ JR., 1993, p. 447).

Oportuno consignar que tanto o precedente como o artigo doutrinário que sustentaram o argumento são antigos, produzidos antes do aparecimento das redes sociais, do armazenamento de dados na nuvem (*cloud*) ou da análise do comportamento de usuários na internet pelas empresas de tecnologia.

Ademais, como já se pontuou na doutrina (MARMELSTEIN, 2019, p. 143), os dados são protegidos pelo art. 5º, inc. X, da CF/ 88, enquanto o sigilo das comunicações está garantido pelo art. 5º, inc. XII. Por outro lado, afirmar que o armazenamento de dados não está sujeito a proteção constitucional é desconhecer a existência e a função do remédio do *habeas data*[3] previsto na Constituição, de forma que, respeitosamente, discorda-se deste pensamento doutrinário.

Em julgamento recente, o STF reviu seu posicionamento sobre o âmbito de proteção constitucional de privacidade. Na Ação Direta de Inconstitucionalidade n° 6387/DF, em

[2] MS 21729, Relator(a): Min. MARCO AURÉLIO, Relator(a) p/ Acórdão: Min. NÉRI DA SILVEIRA, Tribunal Pleno, julgado em 05/10/1995, publicado no DJ 19-10-2001, p. 033. Disponível em: http://stf.jus.br/portal/jurisprudencia/listarJurisprudencia.asp?s1=%28MS%24%2ESCLA%2E+E+21729%2ENUME%2E%29+OU+%28MS%2EACMS%2E+ADJ2+21729%2EACMS%2E%29&base=baseAcordaos&url=http://tinyurl.com/bhlncmt. Acesso em 03.05.2020.

[3] O *habeas data* é um remédio constitucional previsto no artigo 5, inciso LXXII, da Constituição de 1988. Foi criado com o intuito de assegurar o conhecimento de informações relativas à pessoa do impetrante constantes de registros ou bancos de dados de entidades governamentais ou de caráter público e para permitir a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo.

apreciação à Medida Provisória n° 954, o tribunal discutiu o uso de dados pelo Estado e a necessária proteção à privacidade em um momento de emergência sanitária. Neste julgamento, que será analisado detidamente em momento oportuno no presente artigo, o STF aderiu a concepção contemporânea de privacidade que engloba o direito de ser deixado só ou de impedir a intromissão na vida alheia e a possibilidade de o cidadão controlar a circulação e uso de dados pessoais, seja em meios físicos ou digitais.

2. Proteção de dados pessoais no direito brasileiro

O problema de tutelar o armazenamento e o processamento de dados pessoais é que esses dados são armazenados e utilizados, muitas vezes, à revelia dos titulares. Neste cenário, foi editada a Lei 13.709/2018, conhecida como Lei Geral de Proteção de Dados – LGPD, que disciplina a proteção de dados pessoais no Brasil.

O referido diploma normativo estabelece definições legais que são importantes para a análise em curso no presente texto. A LGPD define em seu artigo 5º o que é dado pessoal, dado pessoal sensível, dado anonimizado, titular, banco de dados, controlador, operador, encarregado, anonimização, consentimento e uso compartilhado de dados, dentre outros conceitos relevantes para o direito digital.

O dado pessoal é a informação relacionada a pessoa natural identificada ou identificável (artigo 5º, inciso I, LGPD). O dado pessoal sensível é o dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural (artigo 5º, inciso II, LGPD).

Para o tratamento de dados pessoais o controlador (pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais) ou operador (pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador) devem observar os seguintes requisitos: consentimento prévio do titular dos dados; propósito específico albergado em lei; confidencialidade e segurança; forma e duração do tratamento dos dados pessoais; identificação do controlador; esclarecimentos sobre eventual compartilhamento; *accountability* dos agentes envolvidos; e respeito aos direitos do titular dos dados previsto no artigo 18 da LGPD.

O consentimento prévio do titular é uma forma de garantir o exercício do direito à privacidade consagrado na Constituição de 1988. O consentimento deve ser fornecido de maneira clara pelo titular, por escrito ou outro meio que demonstre a manifestação da vontade do titular (v. g. formulário eletrônico), cabendo ao controlador dos dados o ônus da prova em caso de dúvida sobre a obtenção do consentimento (artigo 8º, *caput*, combinado com o §2º do mesmo artigo, todos da LGPD).

Imperativo consignar que o consentimento pode ser revogado a qualquer tempo, a critério do titular. Em aplicativos de *contact-tracing*, em razão do tipo da intervenção na vida privada que essa tecnologia permite, tal como veremos, o consentimento prévio e sua revogação são especialmente importantes.

O propósito específico albergado em lei, cuida-se do rol legal taxativo previsto no

artigo 7º, da LGPD. No que tange ao controle epidemiológico da Covid-19, duas hipóteses interessam: a que engloba o tratamento de dados pessoais para o cumprimento de obrigação legal ou regulatória pelo controlador (artigo7º, inciso II, da LGPD) e a possibilidade de a administração pública utilizar dados pessoais para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres (artigo7º, inciso III, da LGPD).

A justificativa legal para o compartilhamento de dados pessoais no contexto de combate a pandemia decorre da interpretação sistemática do artigo 7º, incisos II e III da LGPD combinada com o artigo 6º da Lei 13.979/20, a chamada "Lei da Quarentena", que dispõe:

> Artigo 6º É **obrigatório o compartilhamento** entre órgãos e entidades da administração pública federal, estadual, distrital e municipal de **dados essenciais à identificação de pessoas infectadas ou com suspeita de infecção pelo coronavírus**, com a finalidade exclusiva de evitar a sua propagação. (grifos nossos)

Essa obrigação engloba às pessoas jurídicas de direito privado quando os dados forem solicitados por autoridade sanitária (artigo 6, § 1º, Lei da Quarentena). Os esclarecimentos sobre eventual compartilhamento dos dados pessoais com terceiro devem ser informados ao titular dos dados de forma clara e explícita, pois afeta o consentimento.

Deve ficar claro, também, que os dados tratados para a geração de políticas públicas no enfrentamento da pandemia devem ser utilizados apenas para essa finalidade. A confidencialidade e segurança significa que os dados pessoais armazenados pelo controlador ou operador devem ser protegidos da devassa de terceiros, logos esses agentes devem adotar medidas de segurança, técnicas e administrativas, aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. Eventual vazamento de dados sujeita os envolvidos a responsabilização civil nos termos do artigo 42 da LGPD.

A forma e duração do tratamento dos dados pessoais não pode ser por tempo indeterminado, deve ser observada uma limitação do período de conservação dos dados pessoais que será proporcional a finalidade do tratamento. A identificação do controlador é de rigor, o controlador não pode ser anônimo, pois o titular dos dados tem o direito de saber quem toma decisões referentes aos seus dados pessoais, até para tornar possível o exercício do direito à esclarecimentos.

3. A pandemia do Covid-19 e os desafios do controle epidemiológico

Como se sabe, em 11 de março de 2020, a Organização Mundial de Saúde – OMS, órgão vinculado as Organizações das Nações Unidas – ONU, com a função de dirigir e coordenar o trabalho internacional no domínio da saúde, declarou a epidemia de Covid-19 uma pandemia mundial.

A Covid-19 é uma doença causada pelo novo coronavírus – SARS-Cov-2. O epicentro inicial da doença foi na cidade de Wuhan, província de Hubei, na China, em meados de dezembro de 2019, quando centenas de casos de pneumonia aguda de causa des-

conhecida foram reportados por autoridade locais (HUANG *et al.*, 2020, p. 497).

O vírus Sars-Cov-2 apresenta alta transmissibilidade. A doença tem um longo período de incubação, pessoas carregando o vírus, mas assintomáticas, podem contaminar indivíduos sadios. Assim, há duas respostas sanitárias disponíveis. A primeira é vacinar a população. A segunda é prevenir a transmissão da doença entre a população por meio da separação de indivíduos infectados dos indivíduos saudáveis, interrompendo a transmissão ou, ao menos, diminuindo a velocidade de contaminação, de modo a não sobrecarregar o sistema de saúde, especialmente as Unidades de Terapia Intensiva – UTIs.

Felizmente, no que tange a vacinação, houve evolução significativa desde o início da pandemia. Entre vacinas em desenvolvimento clínico e desenvolvimento pré-clínico há, por volta, de 287 imunizantes desenvolvidos por farmacêuticas de diferentes países, conforme informação da Organização Mundial de Saúde – OMS.[4]

Do ponto de vista gerencial, o desafio da vacinação não foi tanto a pesquisa, mas a velocidade da imunização da população ao nível local, regional e mundial. Segundo a diretora da Organização Pan-Americana da Saúde (OPAS), a taxa de vacinação é muita baixa na América Latina enquanto na América do Norte quase 40 % da população já está vacinada.[5] Na prática, há muita discrepância entre cidades, regiões e países no que tange a cobertura vacinal, ao mesmo tempo que o vírus sofre mutações em populações largamente desprotegidas, levando ao surgimento de novas variantes da doença.

Já as medidas de isolamento social para fins de manutenção da saúde pública impõem vários desafios sociais, jurídicos, econômicos e políticos. Todavia, independentemente da forma, extensão ou complexidade do isolamento epidemiológico adotado, fica patente que a efetividade de qualquer medida depende da adesão mínima da população. Não há sistema repressivo capaz de sancionar a desconformidade generalizada do povo.

Ademais, as medidas de controle epidemiológico devem observar um certo grau de escalonamento ou proporcionalidade em relação ao nível de risco de contágio, no qual as medidas mais restritivas são tomadas somente em casos excepcionais. Neste sentido, o desenvolvimento e aplicação de tecnologias de monitoramento e rastreamento digital foram a grande aposta de 2020 para o controle epidemiológico do Covid-19.

Com relativo sucesso no Leste-asiático, a iniciativa de reconstruir a rede de contatos de um indivíduo infectado com outros indivíduos, de maneira rápida e automatizada, sem a necessidade de longas entrevistas individuais, levou ao desenvolvimento de aplicativos de rastreamento de contato pelo mundo com grande rapidez.

4. As tecnologias de monitoramento digital da pandemia do Covid-19 pelo mundo

O *contact-tracing* é uma tecnologia de monitoramento digital que tem o objetivo de rastrear contatos físicos de pessoas infectadas. Este modelo de monitoramento foi

[4] Disponível em: https://www.who.int/publications/m/item/draft-landscape-of-covid-19-candidate-vaccines. Acesso em 17 jun. 2021

[5] Disponível em: https://www.paho.org/pt/noticias/9-6-2021-controle-da-covid-19-nas-americas-levara-anos-se-vacinacao-continuar-em-ritmo. Acesso em 17 jun. 2021.

utilizado na China, Cingapura e na Coréia do Sul com resultados promissores no começo de 2020. O *contact-tracing* via *Bluetooth* também foi adotado como estratégia pelo duopólio Apple-Google (firmas que controlam o mercado de aplicativos para *smartphones*), em uma solução conjunta de rastreamento social no âmbito da luta contra a epidemia de Covid-19 no mundo, conhecida em inglês como *Google Apple Exposure Notification System*.

Os sistemas de *contact-tracing* aplicados ao controle do Covid-19 são baseados, normalmente, na tecnologia *Bluetooth*, mas é possível sistemas de *contact-tracing* utilizarem outros protocolos de comunicação sem fio, como tecnologia *WiFi* e GPS (SHAHROZ *et al.*, 2021, p. 02).

Em linhas gerais, os *smartphones* possuem a funcionalidade *Bluetooth* para conectar-se a outros dispositivos, tais como telefones celulares, computadores, televisores, caixas de som, relógios e pulseiras inteligentes. Com base em um aplicativo específico (v. g. *TraceTogether* de Cingapura), previamente instalado no telefone pelo usuário, cria-se uma rede de contato entre os vários usuários do aplicativo. Esta rede de contato funciona por meio de trocas códigos de identificação anônimos via *Bluetooth* entre os diversos aparelhos.

A tecnologia *Bluetooth*, permite trocas de dados a curta distância, que são computados como contatos pelo aplicativo de rastreamento quando o celular do usuário permuta códigos com outros telefones. A rede de contatos entre os usuários do aplicativo fica registrada. Se algum dos sujeitos da rede for diagnosticado com o Covid-19, é possível rastrear as pessoas que tiveram contato com o infectado e proceder a testes de vírus ou determinar medidas de isolamento.

O *contact-tracing* poder ser um sistema invasivo no que diz respeito à privacidade se não for respeitado o consentimento do usuário, a finalidade específica e o anonimato da pessoa infectada pelo Covid-19. Na China, Índia e Turquia a adesão a sistemas de *contact-tracing* são compulsórias.

O sistema chinês é especialmente invasivo e repressivo, de difícil reprodução em uma democracia constitucional. O sistema *Health Code* é um aplicativo integrado aos *smartphones* na China, de uso obrigatório por toda população. Qualquer pessoa que testar positivo para a Covid-19 receberá a mensagem de alerta no aplicativo. Neste momento, será enviado um alerta a todos aqueles que poderiam estar em perigo devido a um contato prévio rastreado pelo aplicativo. Adicionalmente, considerando que o sistema está integrado ao Sistema de Classificação Social – SCS implementado pelo Partido Comunista da China, a tecnologia permite impor uma quarentena automatizada a todos os cidadãos que tiveram contato com o indivíduo contaminado.

No smartphone é gerado um código *QR Code* colorido, indicando o potencial status de contágio do usuário. Um código verde permite circular livremente em locais públicos, como metrô ou shopping centers, mas também frequentar restaurantes ou pegar um táxi. Um código amarelo implica uma quarentena preventiva de 7 dias, enquanto o código vermelho indica a quarentena padrão de 14 dias.

O *Health Code* é controlado em locais públicos pela polícia, que pode prender aqueles que descumprem a quarentena. A cor atribuída pode mudar não apenas de acordo com a saúde do usuário, mas também, por exemplo, se ele mora em uma área

onde um foco da doença foi identificado. De fato, o código verde é um passe sem o qual a pessoa só pode ficar confinada. O programa foi lançado em 25 de fevereiro de 2020 em 200 cidades chinesas e já foi estendido progressivamente a todo o território chinês (MOZUR; ZHONG & KROLIK, 2020).

Na Europa, a adesão a aplicativos como *Immuni* na Itália, *StopCovid* na França ou *CoronaApp* na Alemanha é voluntária. O que causa preocupação aos ativistas europeus é o caráter centralizados desses bancos de dados, o que facilitaria o uso para finalidades diversas pelos governos e potencializa o risco a privacidade em eventual falha de segurança com o vazamento de dados.

O *contact-tracing* levanta questões importantes sobre o uso de dados pessoais, uma vez que, a partir dos alertas, por mais que a identidade da pessoa seja ocultada, essa informação pode ser reconstruída se a anonimização não for realizada adequadamente. Aconteceu, por exemplo, na Coreia do Sul, onde o sistema *OpenData* permitiu a reidentificação de indivíduos acometidos pelo Covid-19, causando casos de discriminação (GRIZIOTTI, 2020).

A solução utilizada pelo Sistema Único de Saúde – SUS do Brasil, adota o paradigma do aplicativo desenvolvido em conjunto por Apple e Google. Denominado no Brasil como Coronavírus-SUS, o aplicativo é de adesão voluntária e fornecimento gratuito, disponível na loja de aplicativos das desenvolvedoras do *Android* e do IOS.

O desafio para adoção de sistemas de *contact-tracing* no Brasil é a forma como os *smartphones* são utilizados na sociedade brasileira, especialmente nas classes menos favorecidas. Existe alta penetração deste tipo de aparelho no Brasil, quase 70% dos acessos à internet ocorrem por meio de *smartphones* (NAZARENO, 2020, p.12). Entretanto, muitos destes *smartphones* são antigos e não suportam mais atualizações de sistema operacional ou não possuem memória suficiente para utilizar aplicativos sofisticados de *contact-tracing*.

O aumento do consumo no tráfego e, consequentemente, na tarifa cobrada do consumidor também representa uma barreira para o sucesso desta estratégia de rastreamento. Na prática, o monitoramento digital via celulares está restrito a uma fração da população brasileira, com acesso a aparelhos de última geração e capacidade econômica para arcar com o alto custo da internet móvel no país.

Outrossim, uma taxa baixa de utilização também impede que a rede de rastreamento criada a partir do aplicativo seja eficiente. Há estudos que apontam que uma taxa de utilização do aplicativo de rastreamento digital em torno de 25% da população, resulta em baixa densidade informativa. Neste cenário hipotético, quando duas pessoas se encontram aleatoriamente, a chance que as duas pessoas tenham instalado o aplicativo no próprio celular é de apenas 6,25% (SHAHROZ, 2021, p. 04). Para se ter ideia, o aplicativo do SUS teve 61,5 milhões de downloads desde o lançamento, mas somente 2,3 milhões de usuários ativos em fevereiro de 2021, menos de 1% da população brasileira (TAGIAROLI, 2021).

Em 17 de abril de 2020, o presidente da República editou a Medida Provisória nº 954/2020, que dispõe sobre o compartilhamento de dados por empresas de telecomunicações prestadoras de Serviço Telefônico Fixo Comutado e de Serviço Móvel

Pessoal com o IBGE, para fins de suporte à produção estatística oficial durante a emergência sanitária provocada pelo Covid-19.

A iniciativa causou muita controvérsia no ambiente político e jurídico, apesar de prever em seu bojo diversas salvaguardas: dever de sigilo (artigo 3º, inciso I, MP 954/2020), finalidade específica (artigo 3º, inciso II, MP 954/2020); proibição de cessão dos dados a terceiros (artigo 3º, §1º, MP nº 954/2020); divulgação de relatório de impacto à proteção de dados pessoais, nos termos da LGPD (artigo 3º, §2º, MP nº 954/2020); prevenção de danos, com a destruição das informações compartilhadas da base de dados do IBGE, uma vez superada a situação de emergência de saúde pública (artigo 4º, MP nº 954/2020).

Provavelmente a retórica do atual Chefe do Poder Executivo contaminou um debate realmente importante: autodeterminação informativa versus interesse público em acessar dados pessoais para formulação de políticas públicas. No caso em tela, o CFOAB ajuizou ação direta de inconstitucionalidade, com pedido liminar, em face da integralidade dos dispositivos estabelecidos pela Medida Provisória n. 954/2020, por violação direta aos artigos 1º, inciso III e 5º, incisos X e XII da Constituição Federal, os quais asseguram, respectivamente a dignidade da pessoa humana; a inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas; o sigilo dos dados e a autodeterminação informativa.

A medida cautelar foi deferida por maioria na Suprema Corte, vencido o ministro Marco Aurélio, com o intuito de suspender a eficácia da Medida Provisória nº 954/2020, "a fim de prevenir danos irreparáveis à intimidade e ao sigilo da vida privada de mais de uma centena de milhão de usuários dos serviços de telefonia fixa e móvel" (BRASIL, 2021, p. 03).

A despeito da condução errática do governo federal na gestão da pandemia, compete ao julgador, inclusive ao juiz constitucional, cumprir a lei. Neste sentido, chama a atenção que o debate no STF não levou em consideração o artigo 13 da LGPD, que dispõe sobre o acesso a bases de dados pessoais por órgãos de pesquisa na realização de estudos de saúde pública, como paradigma legislativo apto a analisar a proporcionalidade da medida provisória. No próximo tópico, analisaremos criticamente o julgado a partir desta omissão relevante.

5. A medida provisória 954/2020 e o artigo 13 da LGPD

No panorama delineado no presente texto sobre as tecnologias de *contact-tracing*, seria possível sustentar que a medida provisória nº 954/2020, que visava o compartilhamento de dados pessoais dos usuários do serviço telefônico fixo comutado e do serviço móvel pessoal, pelas empresas de telecomunicações com o IBGE, era adequada, necessária e proporcional, haja vista que o rastreamento via aplicativos voluntariamente utilizados não fornecia massa crítica para formulação de políticas públicas e tomada de decisões no âmbito sanitário.

A princípio, políticas públicas são baseadas em evidências. A automatização da coleta e processamento de dados pessoais, tal como prevista na medida legislativa suspensa pelo STF, facilitaria o exame preciso da situação epidemiológica nas diversas regiões do país, permitiria a pesquisa remota e com segurança, e os dados estariam

a cargo de órgão público de renomada *expertise* em estudos estatísticos.

Além disso, há o artigo 13, da LGPD,[6] que disciplina o uso de dados pessoais para estudos em saúde pública, que prevê os seguintes critérios: tratamento exclusivo dentro dos órgãos de pesquisa; finalidade subordinada a realização de estudos e pesquisas na área de saúde; manutenção dos dados em ambiente seguro e controlado, com a utilização de técnicas de anonimização; garantia de anonimato do titular dos dados pessoais; e, possibilidade de regulamentação por parte da autoridade nacional de proteção de dados e das autoridades da área de saúde e sanitárias, no âmbito de suas competências.

Se cotejarmos a regulação do compartilhamento dos dados pessoais previsto na Medida Provisória nº 954/2020 com as disposições do artigo 13 da LGPD, haverá uma simetria consistente, conforme tabela abaixo:

REQUISITOS PARA O COMPARTILHAMENTO (ARTIGO 13, LGPD)	MEDIDA PROVISÓRIA Nº 954/2020
Tratamento exclusivo dentro dos órgãos de pesquisa	Os dados serão utilizados direta e exclusivamente pela Fundação IBGE (art. 2º, §1º).
Finalidade subordinada a realização de estudos e pesquisas na área de saúde	Os dados pessoais serão utilizados para a produção de estatística oficial, com o objetivo de realizar entrevistas em caráter não presencial no âmbito de pesquisas domiciliares (art. 2º, §1º).
Manutenção dos dados em ambiente seguro e controlado, com a utilização de técnicas de anonimização	Não há previsão expressa na medida provisória;
Garantia de anonimato do titular dos dados pessoais	Os dados compartilhados terão caráter sigiloso; não serão utilizados como objeto de certidão ou meio de prova em processo administrativo, fiscal ou judicial; bem como não poderão ser cedidos a terceiros, seja empresas públicas ou privadas ou a órgãos ou entidades da administração pública direta ou indireta de quaisquer dos entes federativos (art. 3º, incisos I e III, combinados com o § 1º do mesmo artigo).
Possibilidade de regulamentação por parte da autoridade nacional de proteção de dados e das autoridades da área de saúde e sanitárias, no âmbito de suas competências.	A medida provisória delega competência regulamentar ao Presidente da Fundação IBGE, ouvida a Agência Nacional de Telecomunicações – ANATEL (art. 2º, § 2º).

[6] Lei Geral de Proteção de Dados – LGPD. Art. 13. Na realização de estudos em saúde pública, os órgãos de pesquisa poderão ter acesso a bases de dados pessoais, que serão tratados exclusivamente dentro do órgão e estritamente para a finalidade de realização de estudos e pesquisas e mantidos em ambiente controlado e seguro, conforme práticas de segurança previstas em regulamento específico e que incluam, sempre que possível, a anonimização ou pseudonimização dos dados, bem como considerem os devidos padrões éticos relacionados a estudos e pesquisas.
§ 1º A divulgação dos resultados ou de qualquer excerto do estudo ou da pesquisa de que trata o caput deste artigo em nenhuma hipótese poderá revelar dados pessoais.
§ 2º O órgão de pesquisa será o responsável pela segurança da informação prevista no caput deste artigo, não permitida, em circunstância alguma, a transferência dos dados a terceiro.
§ 3º O acesso aos dados de que trata este artigo será objeto de regulamentação por parte da autoridade nacional e das autoridades da área de saúde e sanitárias, no âmbito de suas competências.
§ 4º Para os efeitos deste artigo, a pseudonimização é o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro.

O texto da medida provisória poderia ser legalmente questionado em relação a delegação de competência regulamentar ao Presidente da Fundação IBGE, ouvida a Agência Nacional de Telecomunicações – ANATEL, posto que a LGPD não prevê está hipótese. A lei que positivou o direito a autodeterminação de dados prevê possibilidade de regulamentação da Autoridade Nacional de Proteção de Dados – ANPD e das autoridades sanitárias, no âmbito de suas competências. Todavia, tendo em vista a emergência sanitária, a falta de efetividade das soluções de *contact-tracing* no Brasil, seria justificável o acesso do IBGE para produção de estatísticas oficiais sobre a situação da pandemia no Brasil.

Em relação a falta de menção expressa a manutenção dos dados em ambiente seguro e controlado, com a utilização de técnicas de anonimização para proteção dos titulares dos dados pessoais, a omissão não torna a medida provisória inconstitucional em si, pois a LGPD compõe um microssistema de proteção de dados pessoais que supriria a ausência de regulamentação específica na medida provisória. Cuida-se de uma solução hermenêutica relativamente simples. Caso o intérprete almeje uma solução sofisticada, pode recorrer a teoria do diálogo das fontes tão em voga no direito privado brasileiro. Nos dois casos, o resultado será o mesmo, a constitucionalidade material da medida provisória nº 954/2020.

Oportuno consignar, ainda, outras críticas a decisão da Corte constitucional brasileira, que apontam uma inversão da lógica de legitimidade dos atos estatais, pressupondo a má-fé; a falta de aplicação da técnica de interpretação conforme a Constituição (*Verfassungskonforme Auslegung*); e uso de forma vulgar da técnica ou princípio de proporcionalidade teorizada por Robert Alexy (CARINI & MORAIS, 2020, p. 194).

Todavia, do ponto de vista jurídico, a Corte entendeu no julgamento realizado em 07 de maio de 2020, que embora aprovada, ainda não vigorava a LGPD (Lei nº 13.709/2018), que só entrou em vigor em no dia 18 de setembro de 2020. Neste ponto, o Tribunal entendeu que "o fragilizado ambiente protetivo impõe cuidadoso escrutínio sobre medidas como a implementada na MP nº 954/2020" (BRASIL, 2020, p. 03). Para os ministros, como as normas sancionatórias do diploma legislativo que regula a proteção de dados pessoais não estavam em vigor, havia o risco de uso indevido de dados pessoais por agentes públicos sem a devida possibilidade de responsabilização jurídica.

Soma-se debate jurídico, uma profunda sensação de crise institucional no país, com um chefe de Estado com discurso populista, anti-*establishment*, que não perdia uma oportunidade para gerar conflitos com os demais órgãos de Estado. No âmbito da emergência sanitária provocada pelo Covid-19, o presidente da República agiu, no mínimo, de maneira contraditória, ao estimular aglomerações, propagandear medicação sem eficácia comprovada (hidroxicloroquina), dificultar medidas de distanciamento social e evangelizar contra o uso de máscaras de proteção individual em *lives* na internet para os seus correligionários enquanto o sistema de saúde entrava em colapso em várias regiões do Brasil.

Isto posto, cumpre observar que havia uma profunda sensação de incredulidade em relação as intenções do governo federal com a medida de compartilhamento de dados pessoais entre o IBGE e as empresas de telefonia no tribunal, até porque o censo demográfico à cargo da instituição pública de estatística foi suspenso pelo governo

sob a justificativa de restrição orçamentária.[7]

O ministro Roberto Barroso, sem denunciar expressamente o bolsonarismo em seu voto, ponderou sobre os riscos do compartilhamento e utilização de dados pessoais em uma época de campanhas de desinformação, de campanhas de difamação virtuais e *deep fakes* que podem fraudar o debate público e produzir prejuízos irreparáveis aos direitos de personalidade (BRASIL, 2020, p. 47).

A divulgação de medidas governamentais de monitoramento de jornalistas e opositores depôs significativamente contra o Governo Bolsonaro.[8] Neste sentido, o voto da ministra relatora Rosa Weber faz menção a tendência de que mecanismos excepcionais de limitação de direitos permaneçam durante largo período na democracia, inclusive incorporando-se aos instrumentos ditos normais (BRASIL, 2020, p. 18).

6. *Contact-tracing* e a Lei da Quarentena

Ainda no que tange a privacidade, imperativo consignar outra lei de emergência sanitária que não foi devidamente debatida. A denominada Lei da Quarentena, promulgada em 06 de fevereiro de 2020, tem uma vigência temporal aberta, enquanto perdurar o estado de emergência de saúde internacional decorrente da pandemia do Covid-19 (artigo 8º, Lei 13.979/2020). A referida lei também permite o compartilhamento de informações com a finalidade de subsidiar o enfrentamento da doença.

Independentemente do diploma legal em análise ou que venha a ser editado, um ponto que deverá ser respeitado, na máxima extensão possível, são os princípios fundamentais da LGPD, notadamente, consentimento prévio do titular dos dados, finalidade específica do compartilhamento de dados e prazo determinado.

Ainda que exista dispositivo legal autorizando o compartilhamento de dados essenciais à identificação de pessoas infectadas ou com suspeita de infecção pelo coronavírus, com a finalidade exclusiva de evitar a sua propagação, a utilização de dados pessoais para sistemas de monitoramento e rastreamento digital de infectados demanda uma interpretação sistemática da Constituição de 1988, a LGPD e a Lei da Quarentena, o consentimento prévio do titular dos dados.

Neste ponto, compete problematizar a capacidade de consentimento do usuário. Não se trata apenas de consentir ou não, mas fundamentalmente da possibilidade fática de fazê-lo. Em certas situações, a alternativa a não revelação dos dados pessoais costuma ser uma renúncia a determinados bens ou serviços digitais (DONEDA, 2019, p. 298). No fundo, o consentimento de uso de dados pessoais envolve uma questão coletiva, economicamente estrutural. Consentir com um clique não é suficiente.

Uma solução para o impasse em qualquer sistema de *contact-tracing* é facilitar o que os desenvolvedores chamam de *opt-in* / *opt-out*, ou seja, a adesão ao serviço de

[7] Disponível em: https://g1.globo.com/economia/noticia/2021/04/23/sem-orcamento-censo-e-suspenso-mais-uma-vez-entenda-a-importancia-da-pesquisa-e-o-que-acontece-agora.ghtml. Acesso em: 17 jun. 2021.

[8] Disponível em: https://noticias.uol.com.br/colunas/rubens-valente/2020/12/01/lista-monitoramento-redes-sociais-governo-bolsonaro.htm. Acesso em: 17 jun. 2021.

rastreamento. A escolha deve estar ao arbítrio do titular dos dados e ser de fácil operacionalização técnica, sem demandar grandes conhecimentos de tecnologia. Por outro lado, essa adesão deve ser informada, o que levanta questão sobre acesso à internet, alfabetização formal e digital (*digital literacy*) da população brasileira.

Logo, deve haver um deslocamento do debate sobre o consentimento no sentido de permitir a construção empoderada do direito de anuir, para que o cidadão consiga entender o que está sendo feito com seus dados pessoais, para que compreenda os seus direitos. Somente deste modo o cidadão pode avaliar a extensão do impacto das tecnologias em relação as suas próprias liberdades civis.

Isto posto, as políticas públicas de monitoramento da Covid-19 devem ser transversais, o uso de dados pessoais dos cidadãos deve ser acompanhado de iniciativa de educação digital. É dever das autoridades públicas que utilizam qualquer tipo de análise de monitoramento ou rastreamento digital informar ao público como funciona o procedimento de tratamento dos dados, os objetivos do monitoramento / rastreamento e os eventuais riscos decorrentes do processamento de dados pessoais; e, construir um sistema que permita, de fato, o indivíduo a decidir livremente sobre o uso de seus dados pessoais, algo que não se restrinja ao clicar o botão 'concordo' na tela do celular.

7. Conclusão

O arcabouço jurídico que protege a privacidade das pessoas no Brasil incorpora normas constitucionais e infraconstitucionais. O direito à privacidade está explicitamente previsto na Constituição da República Federativa do Brasil, no artigo 5º, inciso X, e, a nosso sentir, incorpora a proteção de dados pessoais armazenado em meios físicos ou digitais.

As tecnologias de monitoramento e rastreamento digital para realizar o controle epidemiológico do covid-19 no Brasil tem amparo jurídico se obedecerem aos seguintes requisitos: objetivo específico, proporcionalidade e empoderamento do indivíduo. A coleta e o processamento de dados pessoais de saúde devem ser estritamente limitados à finalidade de controlar o contágio, de preferência em banco de dado sob responsabilidade das autoridades de saúde para evitar o cruzamento indevido de dados pessoais de saúde, com outros dados controlados por órgãos de Estado, como registros criminais, eleitorais, fiscais e bancários. A pandemia não pode servir de escusa para o agigantamento da capacidade de vigilância do Estado.

O STF, no julgamento da medida cautelar na ADI nº 6387/DF, firmou posição no sentido que legislação adotada no âmbito de emergência sanitária não pode avançar sobre a privacidade dos cidadãos sem salvaguardas abrangentes. Na oportunidade o Tribunal entendeu a MP nº 954/2020 desatende a garantia do devido processo legal (art. 5º, LIV, da CF), na dimensão substantiva, por não oferecer condições de avaliação quanto à sua adequação e necessidade, e por não regular de maneira minimamente segura a proteção dos dados pessoais sensíveis contra acessos não autorizados, vazamentos acidentais ou utilização indevida, seja na transmissão, seja no tratamento ou uso dos dados dos usuários de telefonia.

Com toda vênia a posição garantista da Corte, demonstramos que era possível manter a eficácia da medida legislativa através de uma interpretação sistemática da legislação. Salvo melhor juízo, a decisão pela suspensão da eficácia da MP nº 954/2020 pode ser interpretada como uma rodada do jogo institucional travado entre o STF e o governo Bolsonaro pela supremacia da interpretação constitucional. Neste sentido, o ambiente de crise sistêmica da democracia brasileira parece ter comprometido a capacidade de interação mínima entre o Executivo e o Judiciário na articulação de políticas públicas.

Por fim, deve-se empoderar o indivíduo, a autodeterminação informacional. A capacidade de consentir deve ser o objetivo primário de uma sociedade civilizada. O direito de consentir deve ser o mais efetivo possível, por meio do fornecimento de informações claras, em linguagem simples, sobre o processamento de dados pessoais pelas iniciativas de monitoramento digital. A experiencia do cidadão deve ser facilitada, o desenho de sites e aplicativos de monitoramento e rastreamento deve ser simples, de uso intuitivo e descomplicado, tanto no momento de anuir ao sistema como no momento de revogar o consentimento, sem qualquer tipo obrigatoriedade compulsória, seja de origem legal ou contratual.

Referências

BEÇAK, R. Sobre a origem das normas constitucionais: a identificação do campo ético moral e sua relação com o Direito. In: BEÇAK, R.; VELASCO, I. (org.). **O Direito e o futuro da pessoa**: estudos em homenagem ao professor Antônio Junqueira de Azevedo. São Paulo: Atlas, 2011.

BIONI, B. R. **Proteção de dados pessoais**: a função e os limites do consentimento. Rio de Janeiro: Forense, 2020.

BRADEIS, L.; WARREN, S. The right to privacy. **Harvard Law Review**, v. 04, n. 05, 1890, p. 193–220. Disponível em: https://www.jstor.org/stable/1321160?seq=1#metadata_info_tab_contents. Acesso em: 03 maio 2020.

BRASIL. Supremo Tribunal Federal. **Medida cautelar em ação Direta de Inconstitucionalidade – ADI nº 6.387**. Tribunal pleno. Relatora Ministra Rosa Weber. Julgamento em 07 de maio de 2020. Publicação em 12 de novembro de 2020.

CARINI, L.; MORAIS, F. S. A possibilidade jurídica de rastreamento tecnológico de contatos diante da decisão do STF na ADI 6387. *In* **Direito, governança e novas tecnologias III** [Recurso eletrônico on-line] organização CONPEDI. Rover, A. J. (coord.) *et al.* Florianópolis: CONPEDI, 2020. Disponível em: www.conpedi.org.br. Acesso em: 17 jun. 2021.

COOLEY, T. M. A **Treatise on the Law of Torts or the Wrongs Which Arise Independent of Contract**. Chicago: Callaghan and Company, 1879. Disponível em: https://repository.law.umich.edu/cgi/viewcontent.cgi?article=1010&context=books. Acesso em: 03 maio 2020.

DONEDA, D. **Da privacidade à proteção de dados pessoais**. 2. ed. São Paulo: Thomson Reuters, 2019.

ELSTRIN, D. Israel's Supreme Court Ends Spy Agency Cellphone Tracking Of COVID-19 In-

fections. **National Public Radio**, 1 de março de 2021. Disponível em: https://www.npr.org/sections/coronavirus-live-updates/2021/03/01/972560038/israels-supreme-court-ends-spy-agency-cellphone-tracking-of-covid-19-infections. Acesso em: 17 jun. 2021.

FERRAZ JR., T. S. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. **Revista Da Faculdade De Direito da Universidade de São Paulo**, v. 88, p. 439–459, 1993. Disponível em: http://www.revistas.usp.br/rfdusp/article/view/67231. Acesso em 03.05.2020.

GRIZIOTTI, G. **Covid 19 e rastreamento humano**. Disponível em: http://www.ihu.unisinos.br/78-noticias/598522-covid-19-e-rastreamento-humano. Acesso em: 03 maio 2020.

HASHIM, A. Pakistan using intelligence services to track coronavirus cases. **Al Jazeera**, 24 de abril de 2020. Disponível em: https://www.aljazeera.com/news/2020/4/24/pakistan-using-intelligence-services-to-track-coronavirus-cases. Acesso em: 17 jun. 2021.

HUANG, C. *et al.* Clinical features of patients infected with 2019 novel coronavirus in Wuhan, China. **The Lancet**, Vol. 395, p. 497–506, 2020.

IENCA, M., VAYENA, E. On the responsible use of digital data to tackle the COVID-19 pandemic. **Nat Med**, v. 26, p. 463–464, 2020. Disponível em: https://doi.org/10.1038/s41591-020-0832-5. Acesso em: 28 nov. 2022.

LANDAU, N.; KUBOVICH, Y.; BREINER, J. Israeli Coronavirus Surveillance Explained: Who's Tracking You and What Happens With the Data, **Haaretz**, 18 de março de 2020. Disponível em: https://www.haaretz.com/israel-news/.premium-israeli-coronavirus-surveillance-who-s-tracking-you-and-what-happens-with-the-data-1.8685383. Acesso em: 03 maio 2020.

MARMELSTEIN, G. **Curso de Direitos Fundamentais**. São Paulo: Atlas, 2019.

MILL, J. S. **On liberty**. New Haven: Yale University Press, 2003.

MOZUR, P.; ZHONG, R.; KROLIK, A. In Coronavirus Fight, China Gives Citizens a Color Code, With Red Flags, **The New York Times**, 1.º de março de 2020. Disponível em: https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html. Acesso em 03 maio 2020.

NAZARENO, C. **Aplicativos de celular para rastreamento de contato como estratégia contra a Covid-19 no Brasil**. Brasília: Câmara dos Deputados, 2020.

SHAHROZ, M. *et al.* COVID-19 digital contact tracing applications and techniques: A review post initial deployments. **Transportation Engineering**, v. 5, 2021, p. 1–9. Disponível em : https://doi.org/10.1016/j.treng.2021.100072. Acesso em: 17 jun. 2021.

TAGIAROLI, G. App do SUS que monitora avanço da covid fracassa por falta de uso. **UOL**, 14 de abril de 2021. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2021/04/14/falta-de-politica-nacional-faz-app-do-sus-flopar-no-rastreamento-de-contato.htm. Acesso em: 17 jun. 2021.

TAVARES, A. R. **Curso de direito constitucional**. 17. ed. São Paulo: Saraiva, 2019.

VIEIRA, O. V. **Supremo Tribunal Federal**: jurisprudência política. 2. edição. São Paulo: Ma-

lheiros, 2002.

WILDER-SMITH, A.; FREEDMAN, D. O. Isolation, quarantine, social distancing and Community containment: pivotal role for old-style public health measures in the novel coronavirus (2019-nCoV) outbreak. **Journal of Travel Medicine**, 2020, 1–4.

ZUBOF, S. **The age of surveillance capitalism**: the fight for a human future at the new frontier of power. Londres: Profile Books, 2019.