V. 18 N. 3
2022

ISSN 2317-6172

Revista DIREITO GV

FGV DIREITO SP

Recebido: 26.02.2021
Aprovado: 12.05.2022

https://doi.org/10.1590/2317-6172202232

Proteção de dados pessoais e direito à privacidade no contexto da pandemia de covid-19: uma análise das aplicações de *contact tracing* à luz da proporcionalidade

PROTECTION OF PERSONAL DATA AND RIGHT TO PRIVACY IN THE CONTEXT OF PANDEMICS: AN ANALYSIS OF CONTACT TRACING APPLICATIONS CONSIDERING THE PROPORTIONALITY

Ana Marília Dutra Ferreira da Silva[1], *Carlos Eduardo da Silva*[2], *Mariana de Siqueira*[3] e *KayoVictor Santos Marques*[4]

Resumo

A alta capacidade de disseminação do vírus SARS-CoV-2 fez com que vários países passassem a adotar providências excepcionais. Para assegurar a eficiência na fiscalização do cumprimento dessas determinações, os países começaram a valer-se da tecnologia da informação, entre elas o desenvolvimento de aplicativos de *contact tracing*. O uso dessa tecnologia enseja uma intervenção estatal no direito à privacidade, pois implica o tratamento de dados pessoais, de modo que se questiona a sua constitucionalidade no contexto do ordenamento jurídico brasileiro a partir da análise da sua proporcionalidade. Este trabalho, portanto, objetiva, com base no estado da arte apresentado, identificar os limites legais e constitucionais da utilização dos aplicativos de *contact tracing* pelo Estado brasileiro em um contexto de pandemia à luz do direito à privacidade, em face do conteúdo da LGPD e a partir da aplicação do critério da proporcionalidade. Nesse cenário, questiona-se: diante da colisão entre a proteção aos dados pessoais, o direito à privacidade e a tutela da saúde pública, é proporcional que o Estado faça uso de aplicações de *contact tracing*? A pesquisa fez uso do método dedutivo e pautou-se em uma análise exploratória e interdisciplinar, recorrendo tanto à dogmática jurídico-constitucional quanto ao conhecimento técnico da tecnologia da informação. É possível concluir que as aplicações de *contact tracing* devem ser construídas de modo a seguir o protocolo da descentralização, utilizando uma abordagem baseada em proximidade e técnicas seguras de transmissão de dados e encriptação de informações para facilitar a anonimização dos dados.

Palavras-chave

Aplicativos de rastreamento de contatos; pandemia SARS-CoV-2/covid-19; direito à privacidade; critério da proporcionalidade; proteção de dados pessoais.

Abstract

Several countries are taking exceptional measures to control the high spreading capacity of SARS-CoV-2 virus. In order to ensure efficiency in monitoring compliance with these determinations, countries began to use information technology, including the development of contact tracing applications. However, the use of this technology entails State intervention in the right to privacy, as it implies the processing of personal data, so that its constitutionality is questioned in the context of the Brazilian legal system. In this context, this work aims to identify the legal and constitutional limits in the use of contact tracing applications in a pandemic context by the Brazilian State, taking into consideration the right to privacy and the principle of proportionality. This research applied the deductive method

1 Universidade Potiguar, Natal, Rio Grande do Norte, Brasil
https://orcid.org/0000-0003-0662-1388

2 Sheffield Hallam University, Departamento de Computação, Sheffield, South Yorkshire, Reino Unido
https://orcid.org/0000-0001-9608-439X

3 Universidade Federal do Rio Grande do Norte, Natal, Rio Grande do Norte, Brasil
http://orcid.org/0000-0002-4477-6076

4 Universidade Federal do Rio Grande do Norte, Natal, Rio Grande do Norte, Brasil
https://orcid.org/0000-0002-6696-6065

and was based on an exploratory and interdisciplinary analysis, making use of both legal-constitutional dogmatics and technical knowledge of information technology. Thus, it is possible to conclude that contact tracing applications must be built following a decentralized architecture, using a proximity-based approach and secure data transmission and information encryption techniques to facilitate data anonymization.

Keywords
Contact-tracing applications; SARS-CoV-2/COVID-19 pandemic; privacy rights; principle of proportionality; protection of personal data.

Introdução

A covid-19 é causada pelo vírus SARS-CoV-2, que tem uma alta velocidade de disseminação, de modo que o controle da transmissão desse vírus em humanos se tornou uma questão crucial para vários governos ao redor do mundo. Inúmeras estratégias foram pensadas para mitigar o índice de contaminação, a exemplo da quarentena, do isolamento e distanciamento social, do uso obrigatório de máscaras, da realização de testagem em massa da população, do mapeamento do fluxo de trânsito dos indivíduos e do *contact tracing*, processo de identificação e monitoramento de pessoas expostas ao vírus.

A partir das aplicações de *contact tracing*, é possível identificar as pessoas contaminadas e expostas ao vírus, bem como sua rede de contatos, a fim de realizar as devidas notificações, os respectivos testes e as medidas de isolamento social.

A utilização da tecnologia da informação pelo Estado, como meio de fiscalizar o cumprimento das medidas de isolamento e distanciamento social, desperta um importante debate em torno da tutela do direito à privacidade. Isso porque, para realizar esse controle, governo e empresas teriam acesso aos dados pessoais dos indivíduos. Nesse cenário, investiga-se se a adoção de medidas de monitoramento, através dos aplicativos de *contact tracing*, está em consonância com o princípio da proporcionalidade presente no sistema constitucional brasileiro e com a Lei Geral de Proteção de Dados Pessoais (LGPD).

O presente trabalho objetiva, de maneira geral, compreender os limites da intervenção estatal na garantia fundamental da privacidade no contexto do tratamento de dados pessoais para combater pandemias, a exemplo da causada pela covid-19, a partir da aplicação do critério da proporcionalidade, conforme concebido por Schlink e Pieroth (2012), seguidos por Martins (2012), para quem a proporcionalidade prescinde da análise da proporcionalidade em sentido restrito por ser esta marcada por um viés mais político do que jurídico. Para tanto, a primeira seção se destinará à análise da área de proteção do direito à privacidade com base na doutrina e na legislação. Na segunda seção, será feito um exame da evolução da legislação

concernente à proteção de dados pessoais no Brasil no período posterior à Constituição Federal de 1988 (CF/88).

Por fim, na terceira seção, verificar-se-á se a utilização de aplicativos de *contact tracing* como forma de combater o avanço de pandemias atende ao critério da proporcionalidade. Assim, discutir-se-ão se as formas de tratamento de dados que decorrem dessa tecnologia sobrevivem à análise: (i) da legitimidade/legalidade do propósito e do meio; (ii) da adequação do meio; e (iii) da necessidade do meio utilizado.

A pesquisa pautou-se em uma análise exploratória com a aplicação do método dedutivo. Fez-se uso da doutrina jurídica brasileira, da legislação atinente ao objeto do estudo, bem como de artigos internacionais, os quais ajudaram a dar conta do estado da arte das técnicas de monitoramento de dados pessoais ao redor do mundo.

1. O DIREITO À PRIVACIDADE À LUZ DO ORDENAMENTO JURÍDICO BRASILEIRO

O art. 5º, X, da CF/88 assegura a inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas, e prevê o direito à indenização pelo dano material ou moral decorrente de sua violação. Trata-se de uma garantia inédita, já que as Cartas Constitucionais anteriores restaram omissas quanto a esse direito fundamental.

Da Constituição de 1824 à Constituição de 1967, as garantias que mais se aproximavam do direito à privacidade eram a inviolabilidade do domicílio e da correspondência,[1] as quais também são previstas pela Constituição atualmente vigente. Trata-se, portanto, de um avanço importante, apesar de tardio, já que a Declaração Universal de Direitos Humanos prevê, desde 1948, em seu art. 12, a proteção à vida privada, à honra e à reputação como um direito humano (UNITED..., *s.d.*).

O direito à privacidade não se confunde com a garantia à honra e à imagem. Ambos são direitos de personalidade, no entanto possuem objetos de tutela diferentes. A garantia da inviolabilidade da honra e da imagem está ligada à proteção da reputação, do nome.

Segundo o entendimento proferido pela ministra Cármen Lúcia, no julgamento da Ação Direta de Inconstitucionalidade (ADI) 4.815/DF, o direito à honra é aquele que se projeta a partir da sua formação moral e dos valores que cada um carrega, fazendo a pessoa reconhecida, enquanto o direito à imagem é aquele construído a partir da escolha do que se quer ser.

O direito à privacidade tutela, de modo geral, o controle das informações pessoais advindas da esfera íntima e privada dos indivíduos. É o que a ministra classifica como "o que não

1 Destaque-se que as garantias da inviolabilidade do domicílio e da correspondência foram suspensas pelo Decreto n. 10.358/1942.

se pretende viver senão no espaço mais recolhido daqueles a quem recai a escolha" (BRASIL, 2015, p. 7).

O art. 21 do Código Civil robustece essa garantia constitucional ao reiterar que a vida privada é um direito inviolável e ressaltar que o juiz, a requerimento, poderá determinar as providências necessárias para impedir ou fazer cessar ato que viole esse direito.

Tradicionalmente, entende-se a privacidade como o "direito de estar só" ou de reservar a si aquilo que considera que deve ser tratado exclusivamente na esfera privada. Essa noção de não interferência indevida foi bastante expandida a partir de um artigo de Warren e Brandeis publicado na *Harvard Law Review*, em 1890, sob o título "The Right of Privacy".[2] Segundo os autores, o direito à privacidade refere-se a uma garantia "contra o mundo" e envolve a proteção à propriedade intelectual, a escritos pessoais e à aparência pessoal, bem como a declarações, atos, relações domésticas ou pessoais, etc. (WARREN e BRANDEIS, 1890, p. 213).

Os autores também pressupunham que os indivíduos teriam o domínio de seus dados particulares, e controlariam sua divulgação. De acordo com eles, o direito ("*common law*") assegura a cada indivíduo o direito de determinar qual a medida dos seus pensamentos, sentimentos e emoções que pode ser comunicada aos outros (WARREN e BRANDEIS, 1890, p. 198).

Há que se dizer que a preocupação com a privacidade aumenta junto com a evolução tecnológica. Já naquela época, Warren e Brandeis (1890, p. 195) faziam referência ao modo como a tecnologia começava a interferir no cotidiano das pessoas. Os autores afirmavam que recentes invenções e modelo de negócios chamavam atenção para o próximo passo que deveria ser dado a fim de proteger os indivíduos e apontavam como exemplos das mudanças ocorridas o uso cada vez mais comum de fotos instantâneas e a atuação da mídia por meio das empresas de comunicação.

Ainda sobre a era digital e suas evoluções, Palfrey e Gasser (2011, p. 12-13) explicam que no início da década de 1970 o mundo começou a mudar em uma intensa velocidade. O primeiro *bulletin board system* (conhecido por BBS) permitiu às pessoas – através de um computador primitivo e acesso a linhas telefônicas – trocar documentos, ler notícias e enviar mensagens. Os grupos de *Usenet*, organizados em torno de tópicos de interesse para as comunidades de usuários, tornaram-se comuns no início da década de 1980 e os *e-mails* também começaram a entrar no uso popular (PALFREY e GASSER, 2011, p. 12-13).

2 Apesar de a noção de privacidade ter sido impulsionada com a publicação desse artigo, não há que se olvidar que esse direito é fruto de uma construção histórica, decorrente de centenas de anos de discussão sobre o público e o privado. Como bem aduz De Lorenzi Cancelier (2017, p. 217), antes mesmo da publicação do referido artigo, Thomas McIntyre Cooley, presidente da Suprema Corte de Michigan, já havia cunhado a expressão "the right to be let alone", o direito de ser deixado só.

A *World Wide Web* (mais conhecida como internet) fez seu ingresso em 1991, com *browsers* fáceis de usar e amplamente acessíveis poucos anos depois. Os mecanismos de busca como o Google, portais e *sites* de comércio virtual (Amazon e Mercado Livre) chegaram ao cenário no final da década de 1990, e, na virada do milênio, as primeiras redes sociais e os *blogs* popularizaram-se. A era digital transformou rapidamente o modo como as pessoas vivem e se relacionam umas com as outras e com o mundo que as cerca.

Assim, a evolução da capacidade técnica de coletar, processar e utilizar dados, a qual permitiu uma maior circulação de informações, aumentou a preocupação com a garantia da privacidade e promoveu uma ampliação do seu âmbito de tutela (DE LORENZI CANCELIER, 2017, p. 219).

Ferraz Júnior (1993, p. 441) fundamenta o direito à privacidade no princípio da exclusividade, o qual pretende assegurar a identidade dos indivíduos. Segundo o autor, esse princípio comporta três atributos: "a solidão (donde o desejo de estar só), o segredo (donde a exigência do sigilo) e a autonomia (donde a liberdade de decidir sobre si mesmo como centro emanador de informações)".

Por sua vez, Silva (2005, p. 206) relaciona a privacidade ao direito de ser deixado em paz, bem como à esfera de vida doméstica, familiar, íntima cujas informações decorrentes estão sob controle do indivíduo, e cabe a ele decidir sobre sua comunicação a terceiros.

Tradicionalmente, pois, a garantia da privacidade corresponde ao direito que o indivíduo tem: (i) de não sofrer interferências indevidas na sua esfera privada, ou seja, o direito de não ser incomodado ou de ser deixado só; e (ii) de poder controlar a divulgação das informações de caráter pessoal. Esse controle é comumente denominado autodeterminação informativa.

No julgamento da ADI 6.387,[3] proposta pelo Conselho Federal da Ordem dos Advogados do Brasil e que contestava a constitucionalidade da Medida Provisória n. 954/2020, a Suprema Corte brasileira consagrou a autodeterminação informativa e o direito ao sigilo dos dados como pressupostos do respeito à privacidade, e reconheceu que esta não é uma garantia absoluta, mas que só pode ser afastada a partir de fundamentos sólidos, ou seja, "diante de justificativa consistente e legítima" (BRASIL, 2020, p. 9).

O Supremo Tribunal Federal não negou, portanto, que o direito à privacidade possa ser sopesado com outras garantias constitucionais de mesmo nível hierárquico. O tribunal indicou, no entanto, que o afastamento dessa garantia deve ser feito sobre fundamentos sólidos.

A noção de privacidade tem sido ampliada, aproximando-se de outras garantias individuais, como o direito à igualdade e à não discriminação, à liberdade e ao acesso à informação

3 Outras ADIs, no mesmo sentido, foram propostas pelo PSDB, PSB, PSOL e PCdoB, as quais foram reunidas à ADI 6.387/DF para julgamento.

(FRAZÃO, 2019a, p. 50). Nesse sentido, Mulholland (2018, p. 171) afirma que "o direito à liberdade das escolhas pessoais de caráter existencial" consiste em uma das três concepções sobre o direito à privacidade.

Essa expansão do conceito decorre dos avanços tecnológicos e, por conseguinte, da estruturação de uma sociedade digital, de modo que o raio de influência do direito à privacidade se estende a zonas além do seu núcleo original – a intimidade e o direito de ser deixado só. Isso decorre do fato de as esferas pública e privada do indivíduo estarem conectadas em um mundo virtual. Nesse espaço virtual, inclusive, há uma intensificação e uma facilitação do acesso aos dados pessoais dos sujeitos, tendo em vista que atualmente a proteção dos dados pessoais passa a ocupar papel de destaque como direito fundamental do cidadão e protagoniza discussões em escala global.

2. A sistemática da proteção de dados no Brasil e o direito à privacidade

Na sociedade digital, a proteção do direito à privacidade é viabilizada de modo especial pela garantia do sigilo de dados inserida no art. 5º, XII, da CF/88, segundo o qual "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).

Como grande parte das interações sociais e econômicas ocorrem em ambiente virtual, a internet tornou-se o meio onde se concentra o intercâmbio de informações pessoais. Para não ser excluído desse âmbito da vida social, o usuário da internet deve fornecer invariavelmente informações pessoais. Além de ser necessário repassar uma série de dados para poder integrar uma rede social ou realizar uma transação comercial, por exemplo, cada movimento *on-line* deixa rastros e produz informações que podem ser utilizadas por empresas ou governos para os mais diversos fins. A partir de tais informações insertas em banco de dados, ocorre comumente a criação de perfis de personalidade, a qual permite a classificação dos indivíduos em categorias de acordo com suas preferências, hábitos, características e convicções (CUEVA, 2017, p. 60).

Por isso, não é incomum ouvir dizer que os dados pessoais são a maior riqueza da sociedade do século XXI, o principal insumo de uma *data-driven economy*, economia movida a dados (FRAZÃO, 2019b, p. 333). Após o processamento desses dados, extraem-se informações que podem gerar valor para uma empresa ou grupo político. O constituinte derivado brasileiro, com olhar muito atento para esse contexto, inseriu o inciso LXXIX no art. 5º da CF/88, segundo o qual "é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais" (BRASIL, 1988). A partir de então, a proteção de dados pessoais foi elevada expressamente à categoria de direito fundamental individual e, por consequência, ao patamar de cláusula pétrea constitucional.

A capacidade de controlar o acesso aos dados pessoais surge como uma questão crucial para a defesa da privacidade e das liberdades individuais. Quanto mais difundidas são as informações pessoais de um indivíduo, menos protegida está sua privacidade (DONEDA, 2011, p. 94). Diante do fato de que a participação e a interação no meio digital não são mais uma opção, tornou-se urgente o estabelecimento de um marco regulatório para a tutela desses dados pessoais.

Em 2018, seguindo a tendência internacional de publicação de leis específicas sobre o tema da proteção de dados pessoais e mediante inspiração colhida especialmente na normativa europeia (GDPR), foi promulgada a LGPD, Lei n. 13.709/2018, a qual promoveu um importante avanço na tutela dos dados pessoais no Brasil, apesar de não ser a primeira norma infraconstitucional a tratar da questão. O Código de Defesa do Consumidor, desde sua criação na década de 1990, disciplina os bancos de dados e cadastros dos consumidores e institui o direito de acesso e à correção da informação. Em 2011, a Lei n. 12.414 criou o cadastro positivo, estabelecendo alguns direitos e garantias ao consumidor cadastrado, enquanto a Lei de Acesso à informação, Lei n. 12.527/2011, regulamentou o direito de acesso a dados e informações exercido em face da administração pública. Note-se que esta última se preocupou em garantir a transparência do poder público e não propriamente em tutelar a privacidade do indivíduo, de modo que a tutela dos dados pessoais continuou carecendo de regulamentação específica e atenta ao ambiente virtual.

A Lei n. 12.737/2012 inseriu novos tipos penais no Código Penal (arts. 154-A e 154-B) e tipificou penalmente a conduta de violar os dispositivos pessoais alheios com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita. Aqui, o legislador alça à esfera penal a proteção das informações pessoais, tamanha sua importância.

O Marco Civil da Internet, Lei n. 12.965/2014, também tratou da privacidade dos usuários da internet, bem como de questões relativas a acesso, armazenamento e tratamento dos seus dados, e reiterou a ordem constitucional de sigilo das comunicações e inviolabilidade da vida privada, apesar de permitir o fornecimento de dados pessoais a terceiros, por meio do consentimento livre, expresso e informado ou nas hipóteses previstas em lei (art. 7º, VII). Ressalta-se, ainda, a previsão constitucional do *habeas data* e sua regulamentação pela Lei n. 9.507/1997.

É imprescindível mencionar que o fato de existirem normativas anteriores à LGPD dotadas de potencial de tutela dos dados pessoais não é sinônimo da impertinência do advento dessa nova lei. A expansão da internet, a digitalização da vida e o capitalismo de vigilância são pontos que tornam clara a demanda global e, por consequência lógica, a necessidade nacional de produção de uma normativa adequada à contemporaneidade.

A LGPD, desse modo, atenta à vida digital, inaugura a apresentação legal de conceitos, princípios e garantias na sistemática da proteção de dados, disciplina as formas de tratamento dos dados pessoais, discorre sobre a responsabilização de quem viola o seu conteúdo

normativo e cria regras de segurança e boas práticas que devem ser observadas pelos agentes de tratamento de dados. Assim, notável a sua relevância no contexto de uma sociedade marcada pela cotidiana vida virtual.

Por ser a tutela dos dados pessoais na sociedade digital específica e desafiadora, foi criado um órgão destinado à fiscalização do respeito e cumprimento do texto da LGPD no plano administrativo: a Autoridade Nacional de Proteção de Dados (ANPD), que foi criada com a natureza jurídica de órgão federal por meio da Medida Provisória n. 869/2018, convertida na Lei n. 13.853/2019. Esse órgão também é responsável pela promoção de políticas públicas que viabilizem a construção de uma cultura de proteção de dados no Brasil e pela elaboração de normas regulamentares concernentes à tutela dos dados pessoais e privacidade. É possível, diante da complexidade de determinados casos concretos, que outros órgãos e entes da Administração atuem junto à ANPD no tema da proteção de dados pessoais.

Não se pretende aqui fazer um estudo minucioso da LGPD, mas apontar alguns conceitos e princípios que serão importantes para a análise do objeto deste artigo.[4] O art. 5º da lei em comento diferencia dado pessoal comum do dado pessoal sensível. O primeiro trata tão somente da "informação relacionada à pessoa natural identificada ou identificável" (BRASIL, 2018), enquanto o segundo diz respeito ao "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" (BRASIL, 2018).

Dados como nome, sobrenome, documentos pessoais, data de nascimento, endereço, telefone, *e-mail*, dados de localização, endereço de IP são exemplos de dados pessoais. De outro lado, dados sobre crença religiosa, escolha ideológica ou partidária, orientação sexual, origem étnica, cor da pele, doenças preexistentes são dados pessoais sensíveis.[5] Os dados de saúde, portanto, tendem a receber o rótulo de dados sensíveis, fato que acaba direcionando a eles uma proteção ainda mais delicada.

É possível que informações sobre dados sensíveis de um indivíduo sejam obtidas a partir do cruzamento de dados pessoais. A título de ilustração, o monitoramento de dados de

4 Segundo o art. 3º da LGPD, a lei "aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que: I – a operação de tratamento seja realizada no território nacional; II – a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou III – os dados pessoais objeto do tratamento tenham sido coletados no território nacional" (BRASIL, 2018).

5 Ressalte-se que a Lei n. 12.414/2011 já trazia o conceito de informações sensíveis. Segundo esta, informações sensíveis são "aquelas pertinentes à origem social e étnica, à saúde, à informação genética, à orientação sexual e às convicções políticas, religiosas e filosóficas" (BRASIL, 2011).

localização (GPS) ou de transações na internet podem indicar a convicção religiosa ou ideológica de alguém e, até mesmo, sua origem étnica ou preferência sexual.

Os dados anonimizados, por sua vez, são aqueles que não permitem a identificação do seu titular pela "utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento" (art. 5º, III, da LGPD – BRASIL, 2018). Essas técnicas são cruciais para que não seja feita a relação entre dados e titulares no caso de dados pessoais serem compartilhados.

O art. 6º da LGPD[6] prevê uma série de princípios que deverão ser observados na execução das atividades de tratamento de dados pessoais, entre eles o princípio da finalidade, da adequação e da necessidade. O primeiro exige a elaboração de objetivos legítimos, específicos, explícitos e previamente informados ao titular para que haja tratamento dos dados. O princípio da adequação determina que esse tratamento se coadune com as finalidades fixadas, enquanto a partir do princípio da necessidade se conclui que o tratamento deve limitar-se aos dados indispensáveis ao escopo preestabelecido. É possível aduzir, assim, que o tratamento deve restringir-se ao mínimo necessário para atingir as finalidades previamente especificadas e informadas ao titular, as quais devem ser legítimas e explícitas.

O princípio da transparência assegura ao titular dos dados "informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento" (BRASIL, 2018, art. 6º, VI), ao passo que o princípio da segurança determina a "utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não

• • •

6 "Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: I – finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades; II – adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento; III – necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados; IV – livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais; V – qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento; VI – transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial; VII – segurança: utilização de medidas 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 difusão; VIII – prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais; IX – não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos; X – responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas" (BRASIL, 2018).

autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão" (BRASIL, 2018, art. 6º, VII).

Ligado à ideia de segurança, o princípio da prevenção indica a necessidade de ações ou iniciativas que previnam os danos que possam ocorrer em razão do tratamento de dados pessoais, e o princípio da não discriminação veta a realização de tratamento de dados para fins discriminatórios, ilícitos ou abusivos.

Há que se mencionar, ainda, os princípios do livre acesso, da qualidade dos dados e da responsabilização e prestação de contas, os quais garantem aos titulares dos dados gratuidade e facilidade sobre a forma e a duração do acesso, assim como a integralidade dos dados pessoais, os quais devem ser exatos, claros, relevantes ao tratamento e atualizados, considerando sempre a necessidade e a finalidade do tratamento. Os agentes de tratamento são, por seu lado, responsáveis por esclarecer se medidas eficazes e suficientes foram adotadas para a estrita observância e cumprimento das normas de proteção de dados pessoais.

Um ponto muito importante constante do texto da LGPD e que merece ser destacado aqui por ter total conexão com o tema do enfrentamento da pandemia pelo Estado – por meio de políticas públicas de saúde coletiva – é o do consentimento e da diferença de disciplina legal que recebe em relação ao tratamento de dados pessoais feito pelo poder público e pelos particulares. Se, para o particular, a falta de consentimento para tratamento de dados pessoais é exceção, para o Estado não é bem o que ocorre.

Combinando o art. 7º, III, da LGPD com o seu Capítulo IV, é possível entender que o tratamento de dados pessoais realizado pelas pessoas jurídicas de direito público no âmbito da execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, prescinde de consentimento prévio como regra indispensável. Esse tipo de tratamento de dados pessoais pela administração pública deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público.

Para que esse tratamento de dados pelo Estado ocorra de modo compatível com a LGPD, ainda é preciso que exista o encarregado de dados no âmbito da Administração e que sejam informadas as hipóteses em que, no exercício de suas competências, a Administração realiza o tratamento de dados pessoais. O poder público deve, ainda, fornecer informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a realização do tratamento em veículos de fácil acesso, preferencialmente em seu sítio eletrônico, sob pena de responsabilização.

3. Limites da utilização de dados pessoais no combate à pandemia da covid-19

A pandemia do novo coronavírus trouxe uma série de desafios políticos, sociais, econômicos e jurídicos. A alta capacidade de disseminação do vírus fez com que medidas como isolamento

social, uso obrigatório de máscaras e monitoramento da população fossem adotadas por vários países a fim de evitar o colapso do sistema de saúde.

Tais medidas foram alvo de contestação, sobretudo aquelas relativas ao uso da tecnologia da informação, responsável pelo monitoramento do trânsito dos indivíduos, pois alguns juristas e políticos as enxergam como uma constrição indevida aos direitos e às garantias fundamentais, notadamente à privacidade.[7]

Uma das principais iniciativas tomadas consiste no desenvolvimento de aplicativos de *contact tracing*, destinados a mitigar a contaminação pelo mapeamento da cadeia de transmissão (KLEIMAN e MERKLE, 2020). A ideia é identificar as pessoas que foram expostas ao vírus e sua rede de contatos, e realizar as devidas notificações para a adoção de medidas cabíveis, como o isolamento social e a realização de testes. Diferentemente das técnicas de *contact tracing* tradicionais, o uso de aplicativos possibilita obter também informações sobre o posicionamento de indivíduos, indo além dos objetivos de *contact tracing* original ao permitir fiscalizar o cumprimento, por parte da população, das restrições impostas à locomoção (EAMES e KEELING, 2003).

Diversas abordagens para aplicativos de *contact tracing* podem ser encontradas ao redor do globo (AHMED *et al.*, 2020). Por exemplo, aplicativos desenvolvidos em Singapura (*TraceTogether*) e na França (*StopCovid*) não utilizam dados de geolocalização, empregando tecnologias como o *bluetooth* para a troca de pseudoidentificadores gerados aleatoriamente, que ficam armazenados no próprio dispositivo de cada usuário. A intenção é que o usuário do aplicativo seja notificado caso tenha cruzado com alguém diagnosticado com o coronavírus. Ademais, são aplicativos de uso facultativo, o que pode ser um problema, já que é necessária uma adesão de pelo menos 60% da população para que a iniciativa seja eficaz (MAXWELL, 2020, p. 155).

Na China, por sua vez, a instalação do aplicativo que usa dados de geolocalização tornou-se obrigatória durante a pandemia para quem quisesse circular pelas ruas e foi permitido o acesso aos dados dos usuários sem consentimento prévio, enviando-os em tempo real para autoridades locais (PAWLOTSKY, 2020, p. 2). A Coreia do Sul, um dos primeiros países a utilizar a tecnologia no combate à pandemia, não obrigou o *download* de aplicativos pela população, mas utilizou dados de geolocalização de empresas de telefonia móvel, câmeras de segurança e faturas de cartões de crédito para monitorar a população (DE ROSA, 2020).

7 Segundo Oliva (2020, p. 41), põe-se em risco a privacidade pessoal com o uso de aplicações desse jaez por diversos fatores, entre eles está a evidência de que a maioria dessas aplicações é controladas por companhias privadas de tecnologia que monetizam ao compartilhar os dados pessoais de seus usuários.

Alguns estados brasileiros, notadamente São Paulo e Rio de Janeiro, valeram-se de iniciativas bem menos invasivas à garantia da privacidade e utilizaram "informações de geolocalização agregadas e anônimas de diversos cidadãos" (ZAGANELLI e MAZIERO, 2020, p. 175), cujo objetivo era monitorar o volume de pessoas transitando em determinado local ou região para verificar a adesão ou não às regras de isolamento social. Assim, a partir de mapas de calor, seria possível identificar áreas de aglomerações.

A Medida Provisória n. 954/2020 pretendeu estabelecer um monitoramento da situação da pandemia no país a partir de uma solução que avançaria mais sobre a privacidade dos indivíduos. Isso porque a medida – cuja eficácia foi suspensa imediatamente por decisão da Suprema Corte (ADI 6.387) – determinava o envio, pelas empresas de telecomunicação prestadoras do serviço de telefonia fixa ou móvel, à Fundação IBGE, da relação dos nomes, dos números de telefone e dos endereços de seus consumidores, pessoas físicas ou jurídicas.

Quanto à utilização desses aplicativos, o processo de coleta e manipulação de dados pessoais pode se dar de diferentes maneiras: (i) o modelo de coleta e processamento dos dados pode ser centralizado ou descentralizado (AZAD *et al.*, 2020, p. 3-4); (ii) faz-se uso, em geral, de técnicas baseadas em proximidade, como o *bluetooth*, ou em geolocalização, como GPS, para a obtenção dos respectivos dados (AZAD *et al.*, 2020, p. 1; AHMED *et al.*, 2020, p. 134578); (iii) os dados podem ser anonimizados ou não, como é o caso das técnicas baseadas em geolocalização, cujos dados são considerados pseudonimizados, pois normalmente podem levar à identificação do indivíduo quando cruzados com outros dados.[8]

Questiona-se, assim, se essas formas de tratamento de dados pessoais são compatíveis com o sistema constitucional brasileiro, em especial a partir da lógica da proporcionalidade, e quais os limites legais para sua aplicação. Para responder a tal dúvida, aplica-se o critério da proporcionalidade, conforme concebido por Schlink e Pieroth (2012), seguido por Martins (2012), de modo que se deve analisar: (i) a legitimidade/legalidade do propósito e do meio; (ii) a adequação do meio utilizado; e (iii) a necessidade do meio utilizado.[9]

A partir desse marco teórico, dispensa-se a análise do princípio da proporcionalidade em sentido estrito, como proposto por Alexy (2008). Isso porque se considera que a ponderação

8 Como bem explica Almeida *et al*. (2020, p. 2490), a anonimização é a aplicação de técnicas que inviabilizam a associação direta ou indireta dos dados ao indivíduo, enquanto a pseudonimização "geralmente remove os identificadores e os substitui por um código chave único".

9 Aqui não será feita a análise da proporcionalidade em sentido estrito, pois, consoante afirma Martins (2012, p. 148), "o problema da utilização do 'critério' da proporcionalidade em sentido estrito vai além de sua dúbia objetividade ou potencial subjetividade. Ele tem o condão de ferir tanto o princípio da separação de funções ('poderes') estatais quanto o princípio democrático, pois ponderar em sentido estrito significa tomar decisões políticas e não jurídicas".

feita a partir da aplicação desse princípio "carece de padrões racionais e vinculativos", de modo que a referência a uma ordem de valores limita-se à identificação de um padrão, mas não à comprovação deste (SCHLINK e PIEROTH, 2012, p. 109). Trata-se, portanto, de uma análise subjetiva, pois não existiria uma "medida objetiva, cientificamente comprovada para a ponderação" (MARTINS, 2003, p. 36). Além disso, o critério da proporcionalidade em sentido estrito tem potencial para violar o princípio da separação dos poderes, pois implica a tomada de decisões políticas (MARTINS, 2003, p. 37).

Como visto anteriormente, o direito à privacidade não é um direito absoluto, ou seja, ele nem sempre vai prevalecer em face de outros bens jurídicos constitucionalmente tutelados (Medida Cautelar na ADI 6.387/DF – BRASIL, 2020, p. 9). No caso concreto aqui exposto, a privacidade colide diretamente com o direito à saúde, previsto no art. 196 da CF/88, segundo o qual "a saúde é direito de todos e dever do Estado, garantido 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" (BRASIL, 1988). Evidente, portanto, o dever do poder público de adotar ou permitir e promover a adoção de medidas capazes de mitigar a velocidade de contaminação do SARS-CoV-2, entre elas o uso de dados pessoais, de modo que a finalidade da medida se mostra legítima.

Antes de tratar da legitimidade do meio, é necessário retomar os conceitos de dados pessoais e dados pessoais sensíveis e explicar o tema do consentimento como regra geral na LGPD. Os dados de localização, nome e idade, os dados de identificação, por exemplo, não são dados pessoais sensíveis, de modo que se exige, em regra, o consentimento inequívoco e claro do titular para o tratamento por particular (art. 7º, I, da LGPD). No caso de dados pessoais sensíveis sobre se a pessoa testou positivo ou não para o coronavírus, o tratamento, pelo particular, exigirá o consentimento específico e destacado para finalidades específicas (art. 11, I, da LGPD). Assim, no geral, o meio lícito, no que concerne ao tratamento de dados pessoais por particulares, é aquele que pressupõe o consentimento do indivíduo nos termos legais.

É bem verdade que a LGPD estabelece que o tratamento não carece de consentimento quando for utilizado para a proteção da vida ou da incolumidade física do titular ou de terceiro (art. 7º, VII, da LGPD). Aqui, não existe uma tutela direta da vida ou incolumidade física direta, de modo que permitir o uso de dados, pelos particulares, sem o consentimento seria uma interpretação deveras extensiva do texto legal.

Em relação ao Estado, convém destacar que o consentimento prévio ao tratamento de dados pessoais não é a regra, em especial quando for mantido o interesse público da pessoa jurídica de direito público que manipula os dados e quando o tratamento for realizado para fins de execução de políticas públicas, prestação de serviços públicos e cumprimento de normativa. Nesse caso, deve haver a indicação do encarregado de dados, bem como o respeito aos preceitos da finalidade, da necessidade, da transparência e da autodeterminação informativa.

Conforme afirma Azad *et al*. (2020, p. 3), a utilização de aplicações de *contact tracing* pode ser bem empregada para frear o avanço de uma pandemia. Ocorre que, levando em consideração a tecnologia desenvolvida nos últimos anos, esses aplicativos são aptos a invadir a privacidade de forma singular. Para evitar isso, deve-se criar um protocolo para o uso dessas aplicações que esteja compromissado com a proteção da privacidade e com o consentimento do usuário quando for necessário o compartilhamento de informações. No caso do Brasil, convém ressaltar que a LGPD estimula, como regra, o compartilhamento de dados pelo poder público entre pessoas jurídicas de direito público para fins de execução de políticas públicas.

Tratando-se de empresas privadas, é possível concluir que a utilização de aplicativos de *contact tracing* deve ser voluntária e pressupor o consentimento do usuário para o compartilhamento dos dados. Dessa feita, seria necessária a criação de sistemas confiáveis para que mais pessoas se sentissem à vontade em utilizá-los, o que aumentaria a eficiência desse mecanismo de monitoramento. No que tange ao uso de tais aplicativos pelo Estado brasileiro, a adesão à tecnologia pelo cidadão deveria ser voluntária, e prescindível seu consentimento, para fins de tratamento; devem ser respeitados os demais aspectos da LGPD (adequação, necessidade, transparência, etc.).

Após a análise da legitimidade do propósito e do meio, passa-se ao exame da adequação do meio utilizado. O meio será adequado quando "o estado de coisas conseguido pelo Estado por meio da intervenção e o estado de coisas existente quando o propósito puder ser considerado realizado constituírem uma conexão intermediada por hipóteses comprovadas sobre a realidade" (MARTINS, 2012, p. 143). A medida que limita o direito à privacidade deve ser apta a diminuir o nível de contaminação da covid-19, segundo análise da experiência empírica, não se exigindo nenhuma garantia de resultados.

Como demonstrado anteriormente, o tratamento de dados pode acontecer: (i) de forma centralizada ou descentralizada; (ii) valendo-se de informação sobre proximidade (como o *bluetooth*) ou geolocalização (como o GPS) para a obtenção dos respectivos dados; (iii) pela anonimização de dados ou não.

A adoção de qualquer dessas formas de tratamento é apta a alcançar o objetivo pretendido, o que já foi demonstrado pelo exame da aplicação dessas medidas em nível internacional, que consiste em iniciativa sugerida pela própria Organização Mundial de Saúde (WORLD HEALTY ORGANIZATION, 2021). A diferença está no nível de eficiência da medida e de intervenção no direito fundamental à privacidade, o qual é avaliado a partir do exame de necessidade.

A análise sobre a necessidade do meio utilizado visa barrar avanços indevidos, desnecessários sobre o espaço de proteção do direito fundamental alvo da intervenção estatal. Entre os meios adequados, deve-se aferir qual o menos gravoso, ou seja, apenas o meio que onerar "a liberdade individual com menos intensidade será o necessário" (MARTINS, 2012, p. 146).

No modelo centralizado, cada usuário que utiliza o aplicativo de *contact tracing* se registra em um servidor centralizado, normalmente controlado por uma instituição pública ou privada, o qual mantém as informações de todos os usuários. Cada aparelho que contém o aplicativo emite identificadores randomizados para o servidor central, além de armazenar uma lista dos identificadores com os quais tenha tido contato. Quando uma pessoa testa positivo para alguma doença pandêmica, a exemplo do coronavírus, os identificadores das pessoas que tiveram contato anterior com o infectado são enviados ao sistema central, que identifica qual aparelho está associado a qual identificador, sendo assim capaz de notificar esses usuários para que adotem medidas preventivas (AZAD *et al.*, 2020, p. 4).

O modelo descentralizado não permite que uma entidade central tenha acesso a informações pessoais dos usuários. Contudo, algumas informações continuam sendo enviadas para o servidor central, que funciona apenas como um grande quadro de avisos, uma base de dados para consultas. É o que ocorre nos aplicativos baseados na abordagem desenvolvida em conjunto pela Apple e Google. Nesse modelo, cada dispositivo gera identificadores temporários, baseados em uma chave criptográfica, que são compartilhados com dispositivos que estejam próximos, através da tecnologia *bluetooth*. Cada dispositivo armazena de maneira criptografada a lista de identificadores com os quais teve contato. Quando um usuário é diagnosticado com covid-19, ele pode compartilhar a lista de seus identificadores passados com o servidor central, que, por sua vez, publica essa lista para todos os outros dispositivos. Cada dispositivo então verifica se algum dos identificadores publicados está em sua lista de contatos. Desse modo, não existe como o servidor reconstruir a rede de contatos de um usuário, uma vez que a verificação é realizada em cada dispositivo (AHMED *et al.*, 2020).

Assim, entre o modelo centralizado e o modelo descentralizado, infere-se que o segundo protege melhor o direito fundamental à privacidade, pois evita que as informações dos usuários estejam concentradas em uma base de dados única, de modo que a maior parte delas esteja fragmentada nos aparelhos celulares (POMPEU *et al.*, 2020, p. 11). Nesse sentido, tem-se desenvolvido na Europa o *Decentralized Privacy-Preserving Proximity Tracing* (DP-3T) (VAUDENAY, 2020, p. 399).[10]

Quanto à tecnologia para obtenção dos dados, é necessário comparar o uso do *bluetooth* com o uso do GPS, principais técnicas utilizadas pelos aplicativos de *contact tracing*. Não se pretende proibir o uso de um e de outro, mas verificar qual a tecnologia mais ou menos suscetível de causar danos ao direito à privacidade.

10 Necessário dizer que, apesar de a grande maioria dos trabalhos científicos apontar que o modelo descentralizado protege melhor o direito à privacidade, alguns estudos mostram as ameaças que esse próprio modelo apresenta a essa garantia individual, pois tornaria os indivíduos mais suscetíveis e vulneráveis a ataques virtuais. Para mais detalhes, *vide* Vaudenay (2020). Há que se ressaltar, nesse sentido, que não há modelo imune a riscos, o que se pretende é adotar o sistema que os diminua de forma mais eficaz.

O uso de informações de geolocalização caracteriza-se como medida mais gravosa. Isso porque se vale de dados considerados pseudonimizados, já que as operadoras de telefonia são capazes de fazer a associação deles com a identificação do respectivo titular. Além disso, a centralização desses dados permite obter informações sobre todos os movimentos de um indivíduo e possibilita a realização de inferências e cruzamentos com outras fontes de dados. A centralização desse tipo de dado em uma base única acessada pelo governo ou por empresas configura um sério risco à privacidade do indivíduo.

Nesse contexto, urge pontuar que as gigantes da tecnologia, Google e Apple, baniram o uso do rastreamento da localização nos aplicativos de *contact tracing*, a fim de sanar o problema de compartilhamento de dados pessoais, e decidiram adotar a tecnologia *bluetooth*, em conjunto com uma abordagem descentralizada, como forma de atingir o objetivo de ajudar os governos mundiais no controle da pandemia (O'NEILL, 2020).

Pontua-se, ainda, que as aplicações de *contact tracing* que fazem uso do GPS não são confiáveis para apontar de modo preciso quando os indivíduos estão suficientemente próximos para transmitir uma doença contagiosa como a covid-19, visto que a acurácia de aproximadamente 1,8 metros ou 6 pés é muito baixa (OLIVA, 2020, p. 42).

O uso do *bluetooth*, por sua vez, suporta esse tipo de monitoramento baseado em proximidade de maneira mais eficiente, pois permite auferir a distância entre os dois aparelhos, sabendo assim se uma pessoa contaminada estaria ou não perto da outra (OLIVA, 2020, p. 42). Essa característica, combinada com uma abordagem descentralizada, mantém "a maior parte das informações fragmentada nos celulares e não em uma base de dados única" (POMPEU, 2020, p. 11), atendendo aos princípios da segurança e da prevenção, contidos na LGPD, já que favorece a anonimização dos dados.

De fato, uma abordagem baseada em proximidade se adequa melhor aos propósitos do *contact tracing*, pois o importante é saber se houve contato de uma pessoa com alguém diagnosticado com a doença e não propriamente qual a localização dos indivíduos.

A Google e a Apple juntaram esforços e passaram a oferecer uma biblioteca de código (API) aos governos, que utiliza uma abordagem descentralizada e baseada em proximidade com o uso do *bluetooth* como tecnologia, a fim de que eles desenvolvam aplicativos de *contact tracing*. Assim, permite-se que os celulares pessoais se comuniquem uns com os outros para que uma pessoa saiba se teve contato com determinado indivíduo diagnosticado com a doença (O'NEILL, 2020). No intuito de manter o sigilo dos dados pessoais, utilizam-se identificadores únicos que randomicamente mudam de tempos em tempos. As aplicações baseadas nesse mecanismo são denominadas *proximity tracking* ou, em tradução livre, *rastreadores de proximidade* (OLIVA, 2020, p. 42).

Para tal, impuseram as seguintes orientações: (i) apenas as autoridades de saúde do governo poderão criar os aplicativos; (ii) estes deverão requerer o consentimento do usuário para tratar os respectivos dados pessoais; (iii) um segundo consentimento do usuário deverá ser requerido para o compartilhamento da informação de que ele se encontra infectado; (iv) os

dados coletados deverão ser utilizados para ajudar o sistema de saúde e não poderão ser compartilhados para fins policiais nem de propagandas.

Essas orientações vão ao encontro de outras recomendações encontradas na literatura relacionadas a segurança da informação e desenvolvimento de *software*. Por exemplo, Becker, Li e Starobinski (2019, p. 62) apontam que é necessário assegurar a anonimização dos dados utilizando estratégias como randomização de identificadores, enquanto Azad *et al.* (2020, p. 8) salientam a importância na adoção de técnicas que garantam a encriptação dos dados nos sistemas de armazenamento e transmissão desses dados, independentemente da tecnologia a ser utilizada. É necessário, também, criar mecanismos que destruam esses dados uma vez que a pandemia acabe.

Tais práticas podem colaborar para uma melhor construção das aplicações, dar maior privacidade aos conteúdos dos usuários e minimizar de forma significativa as chances de os dados vazarem ou serem utilizados para outros fins que não sejam direcionados ao combate à pandemia.

Imaginar um sistema cem por cento seguro é utópico. No entanto, as observações feitas neste trabalho permitem aferir que algumas técnicas e modelos levam a uma melhor segurança e anonimização dos dados. Vale dizer que a anonimização é um meio necessário para resguardar a privacidade, pois não permite que os dados que serão utilizados estejam vinculados à identidade do titular, de modo que os objetivos do *contact tracing* sejam alcançados com a menor interferência sobre o espaço de proteção do direito fundamental em comento.

Pontue-se, ainda, a relevância da LGPD na proteção da privacidade dos indivíduos que venham a utilizar esse tipo de aplicativo. Além das questões ligadas ao consentimento e à anonimização, a LGPD apresenta regulamentação importante para tratar das permissões dos aplicativos e do compartilhamento dos dados dos usuários com terceiros, por exemplo.

Alguns aplicativos de *contact tracing* requisitam acesso a mensagens de texto, informações de chamadas telefônicas, números de telefones, câmera, microfone, mídias e arquivos dos aparelhos (AZAD *et al.*, 2020, p. 6-7). Obviamente, trata-se de requisições que ferem os princípios da finalidade, adequação e necessidade previstos no art. 6º da LGPD, mencionados anteriormente. No mesmo estudo, verificou-se que alguns desses aplicativos compartilhavam os dados dos usuários com terceiros não identificados, de modo que aqueles careciam de plena consciência de como os seus dados eram ou têm sido utilizados (AZAD *et al.*, 2020, p. 7), o que viola também os fundamentos da referida lei.

Toda essa discussão técnica pretendeu verificar se os aplicativos de *contact tracing* podem ser considerados meios necessários para o combate à pandemia pelos Estados e, dessa feita, verificar se tais ferramentas respeitam o princípio da proporcionalidade. Como visto, somente o meio que gravar a liberdade individual com menos intensidade e for apto a concretizar os objetivos almejados será o necessário. Para isso, faz-se um exame classificatório para identificar os meios necessários e os desnecessários.

Em suma, o que se pôde verificar é que, no estado da arte atual, para que as aplicações de *contact tracing* sejam consideradas meios necessários, elas devem ser construídas de modo a

seguir o protocolo da descentralização, utilizar uma abordagem baseada em proximidade e valer-se de técnicas seguras de transmissão de dados e encriptação de informações para facilitar a anonimização dos dados. Dessa maneira, elas pouparão ao máximo o direito à privacidade. Como um valor heurístico, a avaliação da necessidade pode variar conforme o surgimento de novos estudos que apontem para um sério risco à autodeterminação informativa, por exemplo.

Conclusão

Crises como a pandemia de covid-19 não repercutem apenas nas esferas política e econômica, mas também pressionam fortemente o sistema jurídico a dar respostas para as mais variadas demandas. Uma delas é o controle das medidas de isolamento ou distanciamento social a partir do tratamento de dados pessoais, inclusive de dados pessoais sensíveis. Ocorre que algumas formas de tratamento de dados esbarram em direitos fundamentais caros às sociedades democráticas, como a garantia à privacidade.

Está-se, assim, diante de um dilema jurídico que envolve, de um lado, a garantia de um direito individual e, de outro, o interesse público da coletividade, que deve guiar os governos na criação de políticas públicas eficientes para combater pandemias. A solução desse dilema deve ser encontrada a partir de uma análise interdisciplinar, jurídica e técnica, como foi feito no presente estudo.

No sistema jurídico brasileiro, a Constituição não estabeleceu nenhuma reserva legal ao direito à privacidade, o qual, a despeito disso, pode colidir com outras garantias de mesma hierarquia constitucional, como o direito à saúde. Apesar de sua importância inequívoca como um dos pilares das sociedades liberais e democráticas, a privacidade não é considerada um valor constitucional absoluto, ao mesmo tempo que não pode ser completamente ignorada sob a justificativa de promoção incondicional do interesse público.

Considerando que na pandemia de covid-19 diversos interesses públicos e privados entraram em constante rota de colisão, escolhendo o específico recorte do uso de aplicativos de *contact tracing* pelo Estado como mecanismo de enfrentamento da pandemia, o estudo investigou a compatibilidade de adoção de tais tecnologias com a proporcionalidade, de modo a verificar sua legitimidade, adequação e necessidade. Foram analisados, ainda, dispositivos da LGPD diretamente aplicáveis ao assunto.

Nesse sentido, a título de conclusões, verificou-se que, para que sejam proporcionais, as aplicações de *contact tracing* devem seguir o protocolo da descentralização, utilizar uma abordagem baseada em proximidade (como a tecnologia *bluetooth*) e valer-se de técnicas seguras de transmissão de dados e encriptação de informações. Além disso, devem ser explicitados os dados que eventualmente precisem ser compartilhados, além da necessária criação de um mecanismo de destruição daquilo que foi coletado durante o estado de pandemia. Tais soluções técnicas, segundo o estado da arte atual, contribuem para resguardar o princípio da privacidade nos termos constitucionais.

Ressalte-se que inexiste atualmente uma solução plenamente segura, de modo que riscos de vazamento de dados ou de violação da anonimização persistem. No entanto, a chance de isso acontecer diminui significativamente com a utilização das técnicas e dos modelos aqui apontados, uma vez que o custo e o esforço necessários para tal violação se tornam proibitivos.

No que se refere à LGPD, a normativa é importante instrumento para o tema, pois disciplina as formas de tratamento dos dados pessoais, estabelece regras de segurança e boas práticas, normas sobre responsabilização dos agentes de tratamento de dados e determina a criação da ANPD. Ademais, apresenta normas específicas sobre a utilização de dados pessoais pelo Estado, de modo a apontar para a regra da prescindibilidade do consentimento em caso de aplicação de *contact tracing* e da imprescindibilidade de serem respeitadas as diretrizes normativas da necessidade e adequação do tratamento, do cumprimento do dever de transparência, da nomeação do encarregado, do respeito ao interesse público e da facultatividade na adesão do cidadão ao aplicativo.

É certo que não se pretendeu esgotar o assunto, mas contribuir com tão fervoroso debate que se espraiou pelo país e que ocupará espaço nos tribunais por tempo considerável.

REFERÊNCIAS

ABELER, Johannes *et al*. COVID-19 Contact Tracing and Data Protection Can Go Together. *JMIR mHealth and uHealth*, [*s.l.*], v. 8, n. 4, p. e19359, 2020.

AHMED, Nadeem *et al*. A Survey of Covid-19 Contact Tracing Apps. *IEEE Access*, [*s.l.*], v. 8, p. 134577--134601, 2020.

ALEXY, Robert. *Constitucionalismo discursivo*. Porto Alegre: Livraria do Advogado, 2008.

ALMEIDA, Bethania de Araujo *et al*. Preservação da privacidade no enfrentamento da covid-19: dados pessoais e a pandemia global. *Ciência & Saúde Coletiva*, [*s.l.*], v. 25, p. 2487-2492, 2020.

AZAD, Muhammad Ajmal *et al*. A First Look at Privacy Analysis of Covid-19 Contact Tracing Mobile Applications. *IEEE Internet of Things Journal*, [*s.l.*], p. 1-12, ago. 2020.

BECKER, Johannes; LI, David; STAROBINSKI, David. Tracking Anonymized Bluetooth Devices. *Sciendo: Proceedings on Privacy Enhancing Technologies*, [*s.l.*], n. 3, p. 50-65, 2019. Disponível em: https://www.researchgate.net/publication/334590931_Tracking_Anonymized_Bluetooth_Devices/

fulltext/5d3308db92851cd04675a469/Tracking-Anonymized-Bluetooth-Devices.pdf. Acesso em: 14 out. 2020.

BRASIL. Supremo Tribunal Federal. *Medida Cautelar na Ação Direta de Inconstitucionalidade 6.387 Distrito Federal*. 7 maio 2020. Relatora: Ministra Rosa Weber. Disponível em: http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADI6387MC.pdf. Acesso em: 25 jul. 2020.

BRASIL. *Lei n. 13.709, de 14 de agosto de 2018*. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 20 jun. 2022.

BRASIL. Supremo Tribunal Federal. *Ação Direta de Inconstitucionalidade 4.815 Distrito Federal*. 10 jun. 2015. Relatora: Ministra Cármen Lúcia. Disponível em: http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=10162709. Acesso em: 14 out. 2020.

BRASIL. *Lei n. 12.414, de 9 de junho de 2011*. Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. Brasília: Presidência da República, 2011. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm. Acesso em: 20 jun. 2022.

BRASIL. *Constituição da República Federativa do Brasil de 1988*. Brasília: Presidência da República, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm. Acesso em: 20 jun. 2022.

CUEVA, Ricardo Villas Bôas. A insuficiente proteção de dados pessoais no Brasil. *Revista de Direito Civil Contemporâneo*, São Paulo: RT, ano 4, v. 13, p. 59-67, out./dez. 2017.

DE LORENZI CANCELIER, Mikhail Vieira. O direito à privacidade hoje: perspectiva histórica e o cenário brasileiro. *Sequência: Estudos Jurídicos e Políticos*, Florianópolis, v. 38, n. 76, p. 213-240, ago. 2017.

DE ROSA, Nicholas. Covid-19: Voice Comment Différents Pays se Servent d'Applications de Traçage. *Ici-radio Canada*, Montréal, 30 abr. 2020. Disponível em: https://ici.radio-canada.ca/nouvelle/1698833/applications-de-tracage-suivi-contacts-coronavirus-geolocalisation-bluetooth-canada-quebec-dans-le-monde. Acesso em: 23 jul. 2020.

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. *Espaço Jurídico Journal of Law [EJJL]*, Joaçaba, v. 12, n. 2, p. 91-108, dez. 2011.

EAMES, Ken; KEELING, Matt. Contact Tracing and Disease Control. *Proceedings of the Royal Society London B*, [*s.l.*], v. 270, p. 2565-2571, 2003. Disponível em: http://doi.org/10.1098/rspb.2003.2554. Acesso em: 20 jun. 2022.

FERRAZ JÚNIOR, Tercio Sampaio. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. *Revista da Faculdade de Direito*, Universidade de São Paulo, v. 88, p. 439-459, 1993.

FRAZÃO, Ana. Objetivos e alcance da Lei Geral de Proteção de Dados. *In*: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (coords.). *A Lei Geral de Proteção de Dados pessoais e suas repercussões no direito brasileiro*. São Paulo: Thomson Reuters Brasil, 2019a. p. 47-61.

FRAZÃO, Ana. Plataformas digitais, *big data* e riscos para os direitos da personalidade. *In*: TEPEDINO, Gustavo; MENEZES, Joyceane Bezerra de (coords.). *Autonomia privada, liberdade existencial e direitos fundamentais*. Belo Horizonte: Fórum, 2019b. p. 333-348.

KLEIMAN, Robert; MERKLE, Colin. Digital Contact Tracing for COVID-19. *Canadian Medical Association Journal*, [*s.l.*], v. 192, n. 24, p. E653-E656, June 2020. Disponível em: https://www.cmaj.ca/content/192/24/E653. Acesso em: 26 set. 2022.

MARTINS, Leonardo. *Liberdade e Estado constitucional*: leitura jurídico-dogmática de uma complexa relação a partir da teoria liberal dos direitos fundamentais. São Paulo: Atlas, 2012.

MARTINS, Leonardo. Proporcionalidade como critério de controle de constitucionalidade: problemas de sua recepção pelo direito e jurisdição constitucional brasileiros. *Cadernos de Direito*, Piracicaba, v. 3, n. 5, p. 15-45, jul./dez. 2003.

MAXWELL, Winston. L'outil de traçage StopCovid: entre inefficacité et proportionnalité. *Légipresse*, [*s.l.*], p. 154-156, abr. 2020.

MULHOLLAND, Caitlin Sampaio. Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da Lei Geral de Proteção de Dados (Lei 13.709/18). *Revista de Direitos e Garantias Fundamentais*, Vitória, v. 19, n. 3, p. 159-180, dez. 2018.

OLIVA, Jennifer. *Surveillance, Privacy, and App Tracking*. Boston, jul. 2020. Disponível em: https://ssrn.com/abstract=3675833. Acesso em: 22 jan. 2021.

O'NEILL, Patrick Howell. Google and Apple Ban Location Tracking in their Contact Tracing Apps. *MIT Technology Review*, [*s.l.*], 4 maio, 2020. Disponível em: https://www.technologyreview.com/2020/05/04/1001060/google-and-apple-lay-out-rules-for-contact-tracing-apps/. Acesso em: 14 out. 2020.

PALFREY, Jon; GASSER, Urs. *Nascidos na era digital*: entendendo a primeira geração dos nativos digitais. Porto Alegre: Artmed, 2011.

PAWLOTSKY, Aurèle. L'utilisation des données personnelles dans le cadre de la lutte contre l'épidemie de Covid-19, un risque pour les droits et libertés? *La Revue des droits de l'homme* (*on-line*), [*s.l.*], p. 1-7, 2020. Disponível em: http://journals.openedition.org/revdh/9059. Acesso em: 13 jul. 2020.

POMPEU, João Cláudio Basso *et al*. *O uso de tecnologia da informação para o enfrentamento à pandemia da covid-19*. Brasília: Ipea, 2020.

SCHLINK, Bernhard; PIEROTH, Bodo. *Direitos fundamentais*. Tradução Antônio Francisco de Sousa e Antônio Franco. São Paulo: Saraiva, 2012. Série IDP.

SILVA, José Afonso da. *Curso de direito constitucional positivo*. São Paulo: Malheiros, 2005.

UNITED NATIONS HUMAN RIGHTS. *Universal Declaration of Human Rights*, *s.d.* Disponível em: https://www.ohchr.org/EN/UDHR/Pages/Language.aspx?LangID=por. Acesso em: 15 jul. 2020.

VAUDENAY, Serge. Analysis of DP3T. *IACR Cryptol ePrint Arch*, Report 2020/399, 2020.

WARREN, Samuel; BRANDEIS, Louis. The Right to Privacy. *Harvard Law Review*, [*s.l.*], v. 4, n. 5, p. 193-220, dez. 1890. Disponível em: https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf. Acesso em: 16 jul. 2020.

WORLD HEALTH ORGANIZATION. *Contact Tracing in the Context of COVID-19*. Fev. 2021. Disponível em: https://www.who.int/publications/i/item/contact-tracing-in-the-context-of-covid-19. Acesso em: 25 jul. 2020.

ZAGANELLI, Margareth Vetis; MAZIERO, Simone Guerra. Uso de dados pessoais como meio de controle da covid-19: desafios do direito à privacidade. *Humanidades e Tecnologia (FINOM)*, [*s.l.*], v. 25, n. 1, p. 169-184, 2020.

Como citar este artigo:

SILVA, Ana Marília Dutra Ferreira da *et al*. Proteção de dados pessoais e direito à privacidade no contexto da pandemia de covid-19: uma análise das aplicações de *contact tracing* à luz da proporcionalidade. *Revista Direito GV*, São Paulo, v. 18, n. 3, set./dez. 2022, e2232. https://doi.org/10.1590/2317-6172202232

Ana Marília Dutra Ferreira da Silva

Mestre em Direito Constitucional pela Universidade Federal do Rio Grande do Norte (UFRN). Doutoranda em Direito pela Université de Montréal e Professora da Universidade Potiguar. Membro-Pesquisadora do Grupo de Estudos do Direito Público da Internet e das Inovações Tecnológicas (GEDI) da UFRN.

anamariliadutra@gmail.com

Carlos Eduardo da Silva

Doutor em Ciência da Computação pela University of Kent, Reino Unido. Senior Lecturer na Sheffield Hallam University, Department of Computing, Reino Unido. Membro-Pesquisador do Grupo de Estudos do Direito Público da Internet e das Inovações Tecnológicas (GEDI) da Universidade Federal do Rio Grande do Norte (UFRN).

c.dasilva@shu.ac.uk

Mariana de Siqueira

Doutora em Direito pela Universidade Federal de Pernambuco (UFPE). Professora Adjunta da Universidade Federal do Rio Grande do Norte (UFRN). Coordenadora do Grupo de Estudos do Direito Público da Internet e das Inovações Tecnológicas (GEDI) da UFRN.

marianadesiqueira@gmail.com

Kayo Victor Santos Marques

Especialista em Direito Administrativo pela Universidade Federal do Rio Grande do Norte (UFRN). Bacharel em Direito pela Universidade Potiguar (UNP) e Tecnólogo em Análise e Desenvolvimento de Sistemas pelo Instituto Federal do Rio Grande do Norte (IFRN). Membro-Pesquisador do Grupo de Estudos do Direito Público da Internet e das Inovações Tecnológicas (GEDI) da UFRN. Advogado.

kayovs.marques@gmail.com