OS DADOS E O VÍRUS: TENSÕES JURÍDICAS EM TORNO DA ADOÇÃO DE TECNOLOGIAS DE COMBATE À COVID-19

Rafael A. F. Zanatta

Diretor da Associação Data Privacy Brasil de Pesquisa. Doutorando pelo Instituto de Energia e Ambiente da Universidade de São Paulo. Mestre (2015) em Direito e Economia pela Universidade de Turim (Itália). Mestre (2014) pela Faculdade de Direito da USP. Alumni do Privacy Law and Policy Course da Universidade de Amsterdam. Foi coordenador do programa de direitos digitais do Instituto Brasileiro de Defesa do Consumidor (2015-2018), líder de projetos do InternetLab (2014-2016) e pesquisador da Escola de Direito da Fundação Getulio Vargas (2013-2014).

Bruno R. Bioni

Diretor da Associação Data Privacy Brasil de Pesquisa. Doutorando em Direito Comercial pela Faculdade de Direito da USP. Mestre (2016) com louvor em Direito Civil da Faculdade de Direito da USP. Foi study visitor do European Data Protection Board/EDPB e do Departamento de Proteção de Dados Pessoais do Conselho da Europa. Foi Bolsista da Fundação de Amparo à Pesquisa de São Paulo (FAPESP) e pesquisador visitante ao Laboratório de Pesquisa do Canadá em Direito e Tecnologia da Universidade de Ottawa (Canadá). Foi pesquisador do Grupo de Pesquisa em Políticas Públicas para Acesso à Informação da Universidade de São Paulo (Projeto de Pesquisa Vigilância e Privacidade).

Clara Iglesias Keller

Pesquisadora Visitante no WZB Berlin Social Sciente Center. Pesquisadora Associada ao Alexander von Humboldt Institute for Internet and Society. Doutora (2019) e Mestre (2011) em Direito Público pela Universidade do Estado do Rio de Janeiro – UERJ (Brasil). L.LM em Direito das Tecnologias da Informação e da Mídia pela London School of Economics and Political Science (2012).

Iasmine L. Favaro

Pesquisadora na Associação Data Privacy Brasil de Pesquisa. Foi bolsista no Programa de Educação Tutorial do Ministério da Educação (2017-2018). Graduanda pela Faculdade de Direito da Universidade de São Paulo (Brasil).

Resumo: O presente artigo apresenta os principais achados do projeto de pesquisa "Os Dados e o Vírus" (que acompanhou e documentou a utilização de tecnologias da informação e de comunicação – TICs para o combate à pandemia da COVID-19). Considerando que esses usos fomentaram o debate sobre a legitimidade dessas tecnologias, o artigo também oferece uma análise, voltada para o caso brasileiro, sobre como o quadro institucional da proteção de dados no país foi afetado pela pauta. São descritas as principais tecnologias baseadas em coleta e tratamento de dados utilizadas em nível global e os principais exemplos de adoção no Brasil. Foram abordadas também as tensões judiciais provocadas por esse usos e pelas tentativas de compartilhamento de dados pessoais no contexto da COVID-19 (Ação Popular nº 1019257-34.2020.8.26.0053 e da ADI 6387). Em seguida, foram

analisados os impactos desses debates e ações judiciais sobre a matéria de proteção de dados no país. Dentre as conclusões, destaca-se o fortalecimento desse quadro institucional, contrariando as preocupações iniciais de que o avanço das tecnologias em questão o enfraquecesse.

Palavras-chave: proteção de dados; rastreamento de contatos; vigilância; COVID-19.

1 Introdução

A pandemia da COVID-19 impactou as relações sociais em escala global e intensificou ainda mais a intermediação da vida em sociedade pela tecnologia. O processo de digitalização massiva e o crescimento de coleta e tratamento de dados pessoais, em desenvolvimento há décadas, revelou-se uma ferramenta em potencial para os governos de todo o mundo, que passaram a utilizar essas tecnologias para enfrentar alguns dos desafios impostos pela crise sanitária.

A necessidade de intervenção governamental para conter a pandemia era dramática. Em pouco mais de um semestre, a COVID-19 tirou a vida de mais de 600 mil pessoas. Somente no Brasil, até setembro de 2020, foram mais de 140 mil mortes (Agência Brasil, 2020). Nesse cenário, as tecnologias da informação e de comunicação - TICs se apresentaram como parte da solução, não apenas para informar e conscientizar a população, mas, também, para monitorar a evolução da doença e influenciar o comportamento social. Contudo, o uso dessas ferramentas não é isento de limites de eficácia e legitimidade, dado que as tecnologias em questão também trazem em si graves ameaças a direitos fundamentais.

Desde março de 2020, as iniciativas de combate à pandemia baseadas em TICs passaram a ser objeto de análise do projeto "Os Dados e o Vírus", da Associação Data Privacy Brasil de Pesquisa. Dentre os diversos usos de tecnologias possíveis (Pollo, 2020), o projeto teve como foco o mapeamento dos principais projetos de uso de dados pessoais para enfrentamento à COVID-19, como mapas de calor criados a partir de dados de ERBs (Estações Rádio-Base), índices de aglomeração criados a partir de dados de localização obtidos por aplicativos de celular e projetos de rastreamento de contato (Farrahi, Emonet & Cebrian, 2014; Altuwaiyan, Hadian & Liang, 2018; Cho, Ippolito & Yu, 2020).

O presente artigo sistematiza os principais achados de pesquisa deste projeto. Especificamente, descrevemos brevemente quais foram as principais tecnologias utilizadas no Brasil e em outros países no combate à pandemia. Olhando especificamente para o caso brasileiro, analisamos também o seu impacto no

quadro institucional da proteção do direito fundamental à privacidade e à proteção de dados pessoais no país.

O texto está estruturado em quatro partes que seguem essa Introdução. Na seção 2, apresentamos as principais tecnologias baseadas em coleta e tratamento de dados utilizadas em nível global e que foram identificadas pelo projeto. Trata-se aqui das técnicas de produção de mapas de calor (focadas em aglomeração e mobilidade das pessoas), técnicas de rastreamento[1] de pessoas por geolocalização e técnicas de rastreamento de contato automatizadas por aplicações de internet.[2] Na seção 3, analisa-se a adoção dessas tecnologias no Brasil, com enfoque na experiência dos índices de isolamento social criado e no projeto do Sistema de Monitoramento Inteligente do Estado de São Paulo. Na seção 3, abordamos as técnicas utilizadas no Brasil. Na seção 4, discutem-se as tensões jurídicas provocadas pelo uso dessas tecnologias e pelas tentativas de compartilhamento de dados pessoais no contexto da COVID-19 – especificamente, o julgamento da Ação Popular nº 1019257-34.2020.8.26.0053 e da ADI 6387 (e apensadas). Na seção 5, oferecemos nossa análise sobre os debates a respeito de proteção de dados em contexto da pandemia de COVID- 19, dando atenção especial às decisões judiciais analisadas na seção anterior. O artigo é encerrado pelas nossas conclusões.

2 Do isolamento ao rastreamento

Desde os primeiros momentos da pandemia, o isolamento e distanciamento social se consagraram como principais estratégias imediatas de combate. Assim, alguns países adotaram o *lockdown*,[3] com medidas de coerção às pessoas que não cumprissem o isolamento, permitindo movimentações apenas para fins essenciais (Guzzetta *et al.*, 2020; Figueiredo *et al.*, 2020). Outros apenas orientaram seus cidadãos ao isolamento social, contando com a iniciativa individual e possibilidade das pessoas se manterem em casa.

1 O *contact tracing*, ou rastreamento de contato, é um processo há muito utilizado pela Saúde Pública. Trata-se da identificação do contato entre uma pessoa infectada por alguma doença transmissível com outras pessoas e consequente isolamento parcial ou total das pessoas que mantiveram esse contato, a fim de diminuir a velocidade de propagação de uma doença infecciosa.

2 No Brasil, aplicações de *internet* são juridicamente definidas como "o conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet". Este conceito aplica-se para *softwares* que transmitem dados *online* e aplicativos de celular. A definição está no Marco Civil da Internet, Art. 5º, inciso VII (Lei 12.965/2014).

3 Aqui entendido como obrigatoriedade formal de isolamento social em domicílio, à exceção das hipóteses de circulação expressamente previstas em lei e regulamento (como, por exemplo, o deslocamento de trabalhadores essenciais, compras e exercício físico).

De acordo com a estratégia adotada, variaram também as ferramentas que as apoiaram. Nessa seção, serão descritas as principais tecnologias de rastreamento e de proximidade adotadas e identificadas pelo projeto "Os Dados e o Vírus". Trata-se, aqui, de análises cartográficas (ou "mapas de calor") e de rastreamento de contato digital, incluídas as suas variações: (i) em relação ao dados usados (por dados de geolocalização ou por proximidade através do uso de *bluetooth*) e (ii) em relação à forma de armazenamento desses dados (modelos centralizado e descentralizado).

2.1 Uso de dados para mapas de calor

As análises cartográficas são feitas a partir do uso de dados de georreferenciados, isto é, dados que descrevem fenômenos geográficos cuja localização está associada a uma posição sobre a superfície terrestre.

Quando um telefone celular realiza uma chamada e emitir um sinal de rádio à torre de telefonia, é possível mensurar o tempo gasto entre o envio e o recebimento de impulsos, medindo, dessa forma, a distância entre o usuário e a torre. Em grandes aglomerados urbanos, esses aparelhos costumam estar entre pelo menos três torres de telefonia, de modo que é possível inferir a localização do telefone que está emitindo as ondas de rádio (Pollo, 2020).

Essa tecnologia pode ser útil para medir, por exemplo, o nível de isolamento social da população de determinada localidade, observando se há circulação desses aparelhos por diferentes bairros ou cidades. A análise agregada de informações de geolocalização permite entender padrões de deslocamento dentro de um espaço geográfico, permitindo inferências sobre deslocamentos entre casa e trabalho, ou entre regiões domiciliares e comerciais. Tal técnica não é isenta de riscos, considerando experiências já demonstradas de identificação pessoal através de estudos de padrões de movimentação de forma iterativa (Thompson & Warzel, 2019).

2.2 A automação do rastreamento de contato

O rastreamento de contato digital se baseia, em linhas gerais, na identificação, através da coleta de dados pessoais, de indivíduos contaminados ou potencialmente contaminados diante de sua proximidade com outro indivíduo contaminado. O rastreamento, em si, não é uma técnica exclusivamente digitalizada, já que ele pode ser feito através de registros, por escrito, de pessoas que estiveram em um determinado lugar, o que também permitiria a sua identificação

e a comunicação diante de riscos de contaminação. É patente, contudo, que a sua execução por via digital, quando acompanhada por adesão suficiente, tem potencial para conduzir esse processo de forma mais rápida, e assim diminuir o número em potencial de contaminação.

Abaixo, descrevemos algumas dessas experiências, divididas conforme a tecnologia utilizada.

2.2.1 Rastreamento por dados de geolocalização

Os *softwares* que utilizam a geolocalização geralmente são executados em segundo plano nos telefones para ajudar com serviços de navegação, e podem rastrear pessoas a cerca de dez metros de sua localização.

Um caso emblemático do uso de geolocalização para rastreamento aconteceu em Taiwan (Chen *et al.*, 2020), depois que três mil pessoas desembarcaram de um navio e, em seguida, algumas testaram positivo para a COVID-19. O governo de Taiwan utilizou os dados de geolocalização individual para procurar eventuais contatos entre seus cidadãos e passageiros.

A tecnologia encontrou mais de seiscentos mil residentes de Taiwan que estavam nas proximidades dos passageiros e os dados de geolocalização dessas pessoas também passaram a ser compulsoriamente coletados. Também foram utilizadas informações como, por exemplo, estabelecimentos onde as pessoas utilizaram cartões de crédito, filmagens de câmeras de segurança e dados telefônicos. Não está claro se esses dados foram eliminados, se ainda compõe bancos de dados no governo de Taiwan ou se esses dados serão utilizados para alguma outra finalidade.

O rastreamento por geolocalização também foi adotado na Noruega. Lá, a Anistia Internacional publicou o relatório "Bahrain, Kuwait and Norway contact tracing apps among most dangerous for privacy"[4] demonstrando que o aplicativo "Smittestopp", usado pelo governo, apresentava alto risco para a privacidade dos cidadãos. Isto porque seu sistema realizava o rastreamento ao vivo da geolocalização dos indivíduos, fazendo upload dos dados de GPS em um servidor central que passou a concentrar informações pessoais de praticamente toda a população norueguesa (Amnesty International, 2020). O relatório apontou que os aplicativos utilizados pela Noruega, bem como os de Bahrein e Kuwait apresentavam um alto grau de invasividade e recomendou que os países interrompessem imediatamente

[4] Fonte: https://www.amnesty.org/en/latest/news/2020/06/bahrain-kuwait-norway-contact-tracing-apps-danger-for-privacy/. Acesso em: 23 set. 2020.

o uso, na medida em que dados pessoais estavam sendo transmitidos em tempo real para o governo (Amnesty International, 2020)

Após o relatório ter sido enviado à autoridade de proteção de dados norueguesa o país deixou de utilizar o rastreamento de contato via GPS e o entendimento da autoridade europeia de proteção de dados (EDPS) foi o de que seria melhor evitar o uso de dados de localização porque estes seriam mais propensos à reidentificação, dando prioridade ao uso de dados de proximidade obtidos através da tecnologia de Bluetooth (EDPS, 2020). Não apenas Taiwan e Noruega fizeram uso do GPS e de dados pessoais individualizados para colocar em prática o rastreamento de contato digital. Foram criados programas governamentais semelhantes na Coreia do Sul, Índia, Islândia, Noruega, Bahrein, Kuwait e em estados dos Estados Unidos, com Dakota do Norte e Utah. O que se demonstrou, no entanto, é que a tecnologia de GPS, além de expor informações pessoais das pessoas, com o rastreamento individualizado, não foi precisa o suficiente para medir distâncias menores que dez metros entre dois celulares. Nesse sentido, o rastreamento seria pouco eficiente para determinar quais encontros foram mais arriscados (Amnesty International, 2020).

2.2.2 Rastreamento por proximidade – Bluetooth

Em sua versão operada através da tecnologia Bluetooth, o rastreamento por proximidade permite que as pessoas que tiveram alguma proximidade troquem "chaves", que são códigos identificadores efêmeros criados pelos aparelhos celulares, renovados em um determinado período de tempo que gira em torno de dez a vinte minutos, num plano de identificação rotativo que minimiza a possibilidade de rastreamento individual. O aplicativo automaticamente notifica as pessoas que tiveram proximidade com infectados, sem que, no entanto, esses dados sejam enviados para uma "central" que realizará o controle. Os usuários podem escolher notificar ou não as agências públicas de saúde em caso de contaminação.

Cingapura foi pioneiro na prática do rastreamento de contato via dados de proximidade por Bluetooth. O aplicativo Trace Together foi aderido pela maior parte da população[5] de Cingapura, com mais de 1 milhão de *downloads* do aplicativo, mas também apresentou problemas relacionados à privacidade, por concentrar os dados de proximidade das pessoas em um servidor central.

[5] Fonte: https://www.straitstimes.com/singapore/about-one-million-people-have-downloaded-the-tracetogether-app-but-more-need-to-do-so-for. Acesso em: 23 set. 2020.

Após a sua adoção em meados de abril, como alternativa ao rastreamento de contato por dados de geolocalização e ao modelo de armazenamento centralizado dos dados, as empresas Apple e Google firmaram uma parceria para desenvolver aplicativos de rastreamento por meio de dados de proximidade. Semelhante ao que aconteceu na Europa, foi utilizada tecnologia Bluetooth Low Energy, ou BLE, uma versão mais moderna e precisa do antigo Bluetooth.

Com a notificação de infecção a um aplicativo de saúde pública, a ferramenta envia os identificadores anônimos conectados aos dispositivos para os servidores centrais do computador. Outros telefones verificam constantemente os servidores centrais quanto aos sinalizadores de transmissão de dispositivos que eles se aproximaram nos últimos quatorze dias e, se houve correspondência, essas pessoas receberão um alerta de que provavelmente entraram em contato com uma pessoa infectada.

A ferramenta, no entanto, apesar de ter sido concebida como alternativa às tecnologias de rastreamento que utilizavam dados de geolocalização e representavam risco mais elevado à privacidade dos usuários, também apresenta algum nível de risco quando se diz respeito à possibilidade de identificação dos usuários. Durante a realização de um teste de vulnerabilidade do aplicativo SwissCovid, que utiliza a tecnologia desenvolvida pelas empresas Apple e Google, foi identificada uma brecha que permitiria fazer a rastreabilidade dos conteúdos relacionados à proximidade de uma pessoa a outra.[6]

3 Técnicas utilizadas no Brasil

Tal como aconteceu em outros países, no Brasil o uso de tecnologias foi uma alternativa prontamente considerada para combater a pandemia de COVID- 19, principalmente em âmbito estadual e local. O primeiro caso no país foi confirmado em 26 de fevereiro de 2020, e já em março foi anunciada uma parceria nesse sentido entre a Prefeitura do Rio de Janeiro e a empresa TIM (Amaral, 2020), acompanhada de outras iniciativas em outras localidades (Nogueira, 2020; G1/PE, 2020). No nível federal, o então Ministério da Ciência, Tecnologia, Inovações e Telecomunicações – MCTIC anunciou a realização de uma parceria com empresas de telefonia para monitorar aglomerações, mas não há notícia de que ela de fato tenha sido implementada (André, 2020).

O anúncio dessas medidas inaugurou o debate brasileiro sobre os limites e legitimidade do uso de tecnologias para combate à COVID- 19. Enquanto alguns

[6] Fonte: https://vimeo.com/453948863. Acesso em: 23 set. 2020.

especialistas e associações da sociedade civil reforçaram os riscos de vigilantismo (Almeida *et al.*, 2020), outras adotaram posições mais temperadas, sem deixar de considerar o respeito a direitos fundamentais. Nesse sentido, a adoção dessas tecnologias seria legítima, inclusive dentro dos termos da própria LGPD, que já teria consagrado os limites devidos para essa utilização de dados (Doneda, 2020; Bioni, Zanatta, Monteiro e Rielli, 2020). Em outros casos, mais do que a legitimidade da medida em si, foi questionada a forma de condução desses processos, em especial, a falta de transparência e informação com a qual esses acordos estavam sendo negociados (Keller e Pereira, 2020).

Nesta seção, serão detalhadas duas das medidas mais significativas adotadas: (i) o Sistema de Monitoramento Inteligente (SIMI) utilizado pelo Governo do Estado de São Paulo a partir de um acordo com empresas de telefonia móvel para o compartilhamento de dados agregados em formato de mapas de calor, e (ii) a tecnologia desenvolvida por uma *startup* brasileira foi aplicada aos estados brasileiros[7] que empregam dados de geolocalização agregados para criar um Índice de Isolamento Social (IIS).

3.1 Emprego de dados de geolocalização agregados

Destaca-se, em primeiro lugar, o uso de dados de geolocalização adotado em diversos estados, através de ferramenta desenvolvida pela empresa InLoco (Endo *et al.*, 2020). A empresa usou dados agregados e anonimizados de geolocalização de mais de 6 milhões de celulares, cruzando-os com dados complementares, como os de Bluetooth e Wi-Fi, a fim de constituir um Índice de Isolamento Social (IIS). A partir disso, criou um mapa dinâmico que mostra quais estados estão cumprindo mais ou menos as medidas de isolamento social.

Segundo a empresa, a API desenvolvida é utilizada em mais de 600 aplicativos comerciais parceiros e que, portanto, para o exercício de sua finalidade comercial, ela coleta e trata dados de mais de 60 milhões de celulares. Dessa forma, a empresa utilizou dados que já eram tratados por ela para desenvolver os mapas de isolamento social.

A empresa afirmou que os dados utilizados são os estritamente necessários para a verificação do índice, que há o consentimento do uso destes e que todos os aplicativos parceiros mencionam explicitamente que haverá compartilhamento de dados com a In Loco. E alega, ainda, que a possibilidade de reidentificação

[7] Fonte: https://mapabrasileirodacovid.inloco.com.br/pt/. Acesso em: 23 set. 2020.

dos dados de georreferenciamento é baixa, pois não há rastreamento de pessoas individualmente.

Apesar de ter encontrado repercussão midiática, a empresa não foi alvo de ação judicial. Comissões de Proteção de Dados Pessoais de algumas Seccionais da Ordem dos Advogados enviaram ofícios à empresa para maiores esclarecimentos, porém nenhuma medida judicial concreta foi tomada contra a adoção do Índice de Isolamento Social. Por unanimidade, a 6ª Câmara de Coordenação e Revisão da Ordem Jurídica Cível Especializada do Ministério Público do Distrito Federal (MPDFT) arquivou um inquérito instaurado em setembro de 2018 para investigar a obtenção de dados pessoais de brasileiros pela In Loco. Após 15 meses de análises, entendeu-se que "a empresa exerce um modelo de negócio que está em conformidade com a legislação vigente, uma vez que não há coleta de dados que permita a vinculação direta ao titular dos dados pessoais" (Medeiros, 2020).

3.2 Emprego de dados provenientes de triangulação de sinal de antenas de operadoras de telefonia (SIMI-SP)

O Sistema de Monitoramento Inteligente de São Paulo (SIMI-SP) foi uma ferramenta desenvolvida pelo Governo do Estado de São Paulo em parceria com empresas de telefonia móvel.[8] Para tanto, as empresas fornecem ao Governo informações de georreferenciamento, mostrando em que lugar se encontram os sinais emitidos pelas antenas dos celulares. Não haveria identificação individual, mas apenas informação sobre quantidade de celulares em determinada região.

As informações são fornecidas pelas empresas de telefonia e usadas na criação de mapas de calor que permitirão inferir (a) o grau de isolamento social da população e (b) ambientes em que há aglomerações de indivíduos. A partir daí, o Governo informa às empresas em quais regiões existe um alto nível de concentração de pessoas ou um baixo nível de isolamento social. As empresas, por sua vez, enviam SMS aos usuários localizados nessas regiões, informando-os sobre a importância do isolamento ou da possível aglomeração de pessoas.

Importante frisar que no SIMI-SP, quem realiza o contato com o usuário e que, portanto, identifica quais pessoas se encontram em qual região são as próprias empresas de telefonia móvel, que já detinham as informações cadastrais

[8] De acordo com o governo de São Paulo, o SIMI-SP é viabilizado por meio de acordo com as operadoras de telefonia Vivo, Claro, Oi e TIM, através da ABR (Associação Brasileira de Recursos em Telecomunicações) e do IPT (Instituto de Pesquisas Tecnológicas). Fonte: https://www.saopaulo.sp.gov.br/coronavirus/isolamento/. Acesso em: 23 set. 2020.

dos usuários. O Governo do Estado não tem acesso a tais dados e tampouco consegue identificar, individualmente, quais pessoas não estão cumprindo o isolamento social. Segundo o Instituto Paulista de Tecnologia – entidade responsável pelo acordo –, "não há recurso ou possibilidade de acesso aos dados pessoais, ou qualquer meio de anular a agregação e anonimização realizada pelas operadoras" (IPT, 2020). Além disso, as operadoras são responsáveis pela segurança da informação de suas bases de dados, aplicando as "premissas da Lei Geral de Proteção de Dados no contexto do acordo de cooperação firmado com o IPT" (IPT, 2020).

Mesmo diante dessa alegada segurança e o não tratamento de dados pessoais, o SIMI-SP foi objeto de diferentes ações judiciais, incluindo um número relevante de Ações Populares. Em parte, as ações ocorreram por motivações políticas, uma vez que atacavam diretamente o governador João Dória após denúncias de opositores políticos – em especial Carlos Bolsonaro e Eduardo Bolsonaro, filhos do Presidente da República Jair Bolsonaro.

3.3 Esquema analítico das técnicas de rastreamento com base nos princípios de proteção de dados

Tão importante quanto descrever quais foram as práticas adotadas de rastreamento, é contrastá-las às normas de proteção de dados pessoais. Com isso, é possível analisar a (des)conformação da adoção e das próprias as narrativas que moldaram tais tecnologias ao direito à proteção de dados pessoais, conforme o quadro a seguir e que está refletido no teste de proporcionalidade do citado relatório "Privacidade e Pandemia" (Bioni *et al.*, 2020):

(Continua)

Quadro 1. Análise das tecnologias de rastreamento à luz dos princípios de proteção de dados

Política de Saúde Pública	Descrição/ Objetivo	Método	Tecnologia	Princípios de Proteção de Dados (Necessidade, adequação, qualidade e segurança)
Isolamento e quarentena (Lei 13.979/2020)	A maneira mais eficiente seria restringir drasticamente a liberdade de locomoção das pessoas. O isolamento se refere à separação de pessoas, meios de transporte e mercadorias para evitar a propagação, resguardadas as atividades essenciais previstas em lei.	Geolocalização individual	GPS e Trinagulação de ERBs	Se a finalidade perseguida é controlar o distanciamento social, o monitoramento da geolocalização individual constante seria desnecessário e inadequado. Além de ser insegura por envolver a formação de uma base de dados mais vulnerável à ataques e usos secundários ilícitos por conter informações de pessoas identificadas (não pseudoanonimizadas).
		Mapas de Calor	Triangulação de ERBs	Se o objetivo é medir o distanciamento social, então o monitoramento da geolocalização de forma agregada seria adequado e necessário. Ainda se a fonte primária dos dados passasse apenas a cartografia desses movimentos e não os dados brutos para a autoridade sanitária, a medida também seria mais segura e menos suscetível a usos secundários ilícitos por conter informações de pessoas não identificadas ou identificáveis (dados anonimizados ou pseudominizados).
			Coordenada de Geolocalização por sinal de Wi-Fi, GPS e etc.	Permitiria medir o distanciamento social com maior precisão em comparação à técnica de triangulação das torres de telefonia. A geolocalização capturada por satélites e outros pontos deteria um raio menor em face daquele mais espaçado das antenas das operadoras de telecomunicações. Com isso, os benefícios desse tipo de monitoramento superariam os demais anteriores por contar dados de mais qualidade.

(Conclusão)

Quadro 1. Análise das tecnologias de rastreamento à luz dos princípios de proteção de dados

Política de Saúde Pública	Descrição/ Objetivo	Método	Tecnologia	Princípios de Proteção de Dados (Necessidade, adequação, qualidade e segurança)
Uso de tecnologias para evitar a propagação da Covid (Lei 13.979/2020)	No contexto de pressão pela retomada das atividades econômicas, seria necessário flexibilizar o distanciamento social mas sem deixar de lado o controle da disseminação do vírus	Rastreamento de Contato	GPS	Se a finalidade é registrar apenas o contato entre as pessoas capazes de disseminar o vírus, então o monitoramento delas de forma constante seria desnecessário e inadequado. Isto porque, registraria até mesmo contatos sem proximidade relevante para fins de contágio.
			Bluetooth centralizado	Se o objetivo é registrar apenas o contato entre as pessoas capazes de disseminar o vírus, então seria adequado e necessário o monitoramento tão somente de quando elas entrassem em uma zona de proximidade relevante para fins de contágio. Isso seria feito justamente através da ativação do Bluetooth, o qual inclusive teria um alto índice de precisão para minimizar ao máximo a retenção de tais informações.
			Bluetooth descentralizado	Ao invés dos dados sobre proximidade de contato serem armazenados em um único lugar e sob controle das autoridades sanitárias, o mais seguro seria que fosse feito no próprio dispositivos das pessoas. Tal segmentação, somada a um descarte automatizado dos dados logo após o período necessário para o vírus se manifestar, minimizaria ainda mais os riscos da atividade de tratamento de dados. Ao fim ao cabo, somente a quantidade de dados estritamente necessária e adequada de dados seria processada.

4 Repercussões jurídicas no Brasil

O contexto institucional da matéria de proteção de dados no Brasil era frágil em fevereiro de 2020, quando a pandemia de COVID-19 chegou ao país. Apesar

da LGPD ter sido aprovada em julho 2018, a maior parte dos seus dispositivos apenas entraria em vigor em julho de 2020. Além disso, assim que a pandemia atingiu o país e o uso de dados como forma de combate surgiu no debate público, iniciou-se, também, um movimento do setor privado para adiar ainda mais a previsão de vigência. Nos meses que se seguiram a fevereiro, a matéria foi objeto de projetos de lei (Keller e Pereira, 2020) e da Medida Provisória 959/2020, que permitia o adiamento para 2021.

Ao mesmo tempo, apesar da criação da ANPD ser prevista na Lei 13.853/2019 (na qual foi convertida a MP 869/2018), não havia qualquer sinal institucional no sentido da sua criação pelo governo federal. A ausência de iniciativa nesse sentido era preocupante, dado que a ANPD cumpre um papel central regulamentação e monitoramento da LGPD, sendo considerada um "pilar fundamental da lei" (Mendes e Doneda, 2018, p. 6).

Diante desse quadro, a chegada de uma grave emergência sanitária, que poderia potencialmente ser combatida com o uso de tecnologias baseadas em coleta e tratamento de dados, de fato acendeu um alerta para a sociedade civil e academia já engajadas na matéria. De um lado, havia uma situação extrema, que abriu espaço para o uso dessas tecnologias até em países com um arcabouço mais amadurecido de proteção de dados. Do outro, a fragilidade do quadro brasileiro era latente, e assim chegou a inspirar previsões mais pessimistas sobre instalação ampla e permanente dessas tecnologias (Barilli, 2020; Requião, 2020).

Nesse contexto, a judicialização das medidas governamentais envolvendo o uso de dados se apresentou como o palco das disputas que se deram sobre a aplicabilidade e extensão dos direitos já previstos na LGPD, mas ainda não vigentes[9]. Nessa seção, destacamos dois julgamentos simbólicos desse movimento, com especial atenção ao julgamento da ADI 6387 e apensadas no Supremo Tribunal Federal – STF.

4.1 A judicialização do SIMI-SP

A implementação do SIMI-SP, foi questionada através de ação popular impetrada por um grupo de advogados.[10] Alegava-se que os termos da parceria entre o Estado de São Paulo e as empresas de telefonia móvel (Claro, Oi, Tim e Vivo) não estavam claros e, principalmente, não haviam sido publicados nos Diário Oficial

[9] Sendo possível traçar um paralelo com o caso israelense, em que importância da atuação do judiciário teria sido potencializada por um contexto de fragilidade institucional, desprovido de um órgão supervisor especializado (Elkin-Koren, 2020).

[10] Ação Popular nº 1019257-34.2020.8.26.0053.

ou na mídia. Tais informações são fundamentais ao juízo sobre proporcionalidade, finalidade e devido propósito do uso de dados, princípios basilares que guiam a matéria e dos quais dependeria a legitimidade de medidas como o SIMI-SP (Mendes e Doneda 2018).

Assim, tal parceria feriria o princípio da publicidade dos atos administrativos, previsto no art. 37 da Constituição Federal e que reconhece a todos "o direito de receber, dos órgãos públicos, informações do seu interesse particular ou de interesse coletivo ou geral" (Medauar, 2018, p. 125). Nesse sentido, a petição inicial destacava que "uma vez que tal parceria público-privada e seus termos não foram divulgados no Diário Oficial do Estado de São Paulo, bem como não conta com a anuência prévia e expressa dos milhões de usuários de telefonia móvel" (Vipiana, 2020).

Além de centrada no desrespeito ao princípio da publicidade, a ação questionou também a ausência de consentimento para a utilização dos dados da população que estaria sendo rastreada sem o devido conhecimento e consentimento para tanto. Por fim, foi alegado que o sistema adotado pelo Governo do Estado de São Paulo estaria ferindo o direito à liberdade de locomoção[11] (CF, art. 5º, XV), uma vez que as pessoas estariam sendo coagidas a permanecer em suas residências, sob risco de sofrerem sanções.

A decisão em primeira instância[12] acatou parcialmente os pedidos dos advogados, determinando que o Governo do Estado de São Paulo apresentasse, no período de dez dias, os termos da parceria firmada com as empresas de telefonia móvel.

A legalidade do SIMI-SP também foi apreciada pelo Superior Tribunal de Justiça (STJ), em Habeas Corpus[13] julgado pela Ministra Laurita Vaz, que entendeu que não havia qualquer risco ou ferimento do direito à privacidade, tampouco perigo ou restrição à liberdade de locomoção, uma vez que a análise de dados não se dava de modo individualizado e as informações eram observadas de forma aglutinada, a fim de aprimorar as medidas de isolamento social para enfrentamento do coronavírus.

[11] Esse foi, por exemplo, o voto do relator (Des. Antonio Carlos Malheiro) vencido no julgamento do Mandado de Segurança nº 2073723-23.2020.8.26.0000: " Entende este relator que, qualquer ação que venha a interferir ou, como no caso, monitorar o direito de ir e vir do cidadão, principalmente, quando esta ação se utilizar da invasão à inviolabilidade dos meios individuais de comunicação, somente poderá ser realizada por meio de autorização judicial, pois é assim que a nossa lei maior determina".

[12] Decisão disponível em: https://www.conjur.com.br/dl/liminar-monitoramento-celulares.pdf. Acesso em: 23 set. 2020.

[13] Habeas Corpus nº 572.996 – SP. Disponível em: https://www.jota.info/wp-content/uploads/2020/04/hc-572-996.pdf>

Algumas outras ações foram interpostas por usuários contra o SIMI-SP ao longo do tempo e parte dos julgados concedeu exclusão do sistema (Gomes, 2020), enquanto outra parte alegou que a própria identificação para fins de exclusão representaria risco à privacidade.[14]

As Ações Populares geraram uma espécie de força-tarefa na Procuradoria do Estado de São Paulo, responsável por promover a defesa do Estado em juízo em razão de ações judiciais. Rapidamente, os procuradores foram capazes de mobilizar a Lei Geral de Proteção de Dados Pessoais em favor do SIMI-SP, trabalhando com conceitos de "anonimização" e com "base legal" para tratamento dos dados pessoais. Nesse sentido, é possível afirmar que as ações mobilizaram os procuradores sobre a importância da LGPD, uma vez que passaram a elaborar estratégias de defesa para o uso legal do SIMI-SP, de acordo com o regramento de proteção de dados pessoais no Brasil.

Apesar de algumas ações terem tido seu pleito negado ou apenas parcialmente provido, é possível afirmar que elas tiveram um efeito positivo sobre o debate público e o quadro institucional da proteção de dados. Isto porque permitiram um maior escrutínio, não apenas judicial, mas também público, dos problemas relacionados à falta de transparência do SIMI-SP e os seus impactos concretos sobre os direitos individuais e coletivos que se relacionam com a proteção de dados.

4.2 ADIs contra a MP 954/2020

O Governo Federal brasileiro editou, em abril de 2020, a MP 954/2020 que obrigava as empresas de telecomunicações a compartilharem dados cadastrais de usuários com o Instituto Brasileiro de Geografia e Estatística (IBGE). A justificativa para a medida era de que, devido à pandemia e ao isolamento social, o Instituto estaria impedido de realizar a pesquisa presencial e, portanto, estabelecer pesquisa estatística oficial. A MP previa que os dados cadastrais seriam manipulados apenas durante o período de emergência pública e vedava o compartilhamento dessas informações com terceiros.

A medida foi amplamente criticada e contestada judicialmente (Palhares *et al.*, 2020). Ações direta de inconstitucionalidade foram impetradas pelo Conselho Federal da Ordem dos Advogados do Brasil – CFOAB (ADI 6387), pelo Partido da Social Democracia Brasileiro – PSDB (ADI 6388), pelo Partido Socialista Brasileiro – PSB (ADI 6389), pelo Partido Socialismo Liberdade – PSOL (ADI 6390) e pelo

[14] Mandado de Segurança Cível nº 2069736-76.2020.8.26.0000.

Partido Comunista do Brasil – PC do B (ADI 6393). Em síntese, as ADIs destacaram (i) o caráter genérico da norma, sem detalhamento da sua finalidade, (ii) a desproporcionalidade entre os dados necessários para a pesquisa amostral visada e a imposição de compartilhamento de dados de milhões de brasileiros e (iii) a previsão de um relatório de impacto à proteção de dados posterior, ao invés de anterior ao compartilhamento e processamento dos mesmos (Mendes e Fonseca, 2020).

A Ministra Relatora Rosa Weber, decidiu, em sede liminar, pela suspensão dos efeitos da MP 954/2020, apontando que as informações que eram objeto do compartilhamento estavam no âmbito constitucional da proteção ao direito à intimidade e à vida privada. No julgamento do mérito, foi reafirmada essa decisão, que seguida pela maioria dos Ministros da Corte, resultou na declaração de inconstitucionalidade da MP 954/2020.

Neste emblemático julgamento, foi a primeira vez que o STF reconheceu expressamente um direito fundamental à proteção de dados pessoais diretamente extraível da Constituição e que demandaria prestações positivas por parte do Estado[15]. Nesse sentido, a decisão consignou, ainda, a omissão do poder público ao não estabelecer a ANPD prevista em lei (Mendes, 2020).

Até então, a Suprema Corte vinha decidindo casos sobre proteção de dados pessoais baseado na lógica do direito à privacidade. Isto é, considerando que a Constituição tutelaria apenas dados sigilosos e a conservação da sua natureza confidencial. No REs 601314,[16] por exemplo, decidiu-se ser lícito o acesso, sem a necessidade de ordem judicial, por parte da Receita Federal, aos dados de transações financeiras junto aos Bancos. O argumento central nesses casos foi que tais informações não deixariam de ser sigilosas, uma vez que seriam manipulados em ambiente controlado e, sobretudo por instituições cujos servidores-membros teriam um dever fiduciário em não publicizá-los. Além disso, não seriam dados sensíveis (de alto grau de intimidade) sobre os indivíduos (*e.g.*, religião, orientação político-partidária), o que tornaria proporcional tal tipo de interferência diante do interesse público a ser ponderado, qual seja, o combate a ilícitos.

Em sentido contrário, o novo precedente passa a não limitar a proteção constitucional ao caráter sigiloso de uma informação. Basta que um dado seja

[15] V. o voto do Ministro Gilmar Mendes, ADI 6387, j. 07/05/2020.

[16] O foco do julgamento é o direito ao sigilo de dados, como se depreende do seguinte trecho: "Do ponto de vista da autonomia individual, o sigilo bancário é uma das expressões do direito de personalidade que se traduz em ter suas atividades e informações bancárias livres de ingerências ou ofensas, qualificadas como arbitrárias ou ilegais, de quem quer que seja, inclusive do Estado ou da própria instituição financeira" (BRASIL, Supremo Tribunal Federal. Recurso Extraordinário 601314. Rel. Min. Edson Fachin, Tribunal Pleno, julgado em 24.2.2016, *DJe* 16.9.2016).

um bem da personalidade – pessoal – para atrair a proteção constitucional (Bioni, 2020). Reconheceu-se, assim, o direito à proteção de dados pessoais como direito autônomo (Bioni & Leite Monteiro, 2020). Nessa linha, o mero tratamento de dados pessoais, seja ele qual for, traz riscos aos titulares desses dados. Por isso, deve ser ancorado em salvaguardas adequadas, que possam mitigar os potenciais efeitos colaterais adversos.

Dessa forma, a proteção de dados pessoais deve receber a mesma proteção conferida pela cláusula do devido processo legal, a partir da ideia de que ao indivíduo deve ser conferido um mínimo de controle contra exposições indevidas de seus dados (Bioni & Martins, 2020). É o que argumentou o Ministro Gilmar Mendes, ao mencionar o "devido processo informacional" e a teoria de Julie E. Cohen (2013), segundo a qual "o caráter autônomo da privacidade sugere uma necessidade de repensar a concepção do devido processo como uma tomada de decisão individualizada", i.e., "[o] devido processo na era de computação abrangente deve pressupor limites à personalização nos processos administrativos públicos".[17]

A decisão pode ser lida como um caso bem sucedido de litígio estratégico que acontece quando da "utilização de arenas de litigância de forma estratégica buscando um impacto que transcenda as partes do caso e contribua para os direitos humanos e a justiça social" (Gomes, 2019). De fato, no julgamento das ADIs, os efeitos da decisão transcendem o governo federal e as entidades autoras da ação, além do objeto imediato das ações. Além da invalidação da MP 954/2020, o julgamento gerou efeitos diversos para o quadro institucional da proteção de dados no país. Enquanto alguns desses efeitos são mais concretos – como o reconhecimento do *status* constitucional da proteção de dados e a consignação da omissão estatal ao não criar a ANPD – outros têm caráter mais abstrato ou simbólico que também são relevantes. Nesse sentido, destacamos, por exemplo, o potencial da retórica da proteção de dados construída dentro dos autos pelos Ministros,[18] entidades que ingressaram as ações e pelas que atuaram como *amicus curiae.*

Fora dos autos, o papel da academia e do terceiro setor também já foi reconhecido (Fernandes, 2020), e se reflete não apenas no resultado do julgamento, como também nas suas circunstâncias. Vale notar que a ação foi pautada para julgamento em velocidade considerável – entre ingresso e julgamento, passou-se menos de um mês –, o que pode indicar uma resposta a essa movimentação.

[17] V. o voto do Ministro Gilmar Mendes, ADI 6387, j. 07/05/2020.

[18] Destaca-se o voto da Ministra Relatora Rosa Weber, que fez um exercício interpretativo relevante ao extrair da Constituição Federal o direito à proteção de dados, e o voto do Ministro Gilmar Mendes, que reconheceu obrigação positiva do Estado de garantir a efetiva proteção e fruição desses direitos fundamentais.

Também é possível cogitar que essa velocidade tenha sido uma resposta à crise sanitária. Contudo, há indícios de que a atuação do STF em contextos de crise pende para a deferência e prudência diante das ações de outros poderes (Leal, 2020) – ou seja, justamente o contrário do que aconteceu nesse caso.

Independente disso, tanto por seus efeitos formais, quanto pelos abstratos, a decisão constitui avanço significativo dos *standards* de proteção de dados pessoais no Brasil, alcançado em meio a uma grande tensão jurídica e política. A partir da "constitucionalização" da proteção de dados pessoais no Brasil, é certo que a decisão pautará governo e tribunais daqui para frente, inclusive em relação a futuras adoções de tecnologias para o combate à COVID-19.

5 Análise

A caminho do encerramento deste artigo, partimos para análise dos fatos e argumentos sobre os quais o projeto "Os Dados e o Vírus" se debruçou, descritos em síntese até aqui.

Conforme a pandemia de COVID-19 se espalhou pelo globo, governos que se posicionam em pontos diversos do espectro político recorreram ao uso de tecnologias para auxiliar o combate ao vírus. Uma reação talvez inevitável, diante dos desafios extraordinários de se governar diante de uma pandemia - representados por risco de perda de vidas em massa, além dos graves riscos econômicos e sociais (Yeung, 2020). Nesse cenário, a adoção de diferentes ferramentas – que impuseram, entre si, diferentes graus de ameaça a direito fundamentais – provocou a atuação da academia e da sociedade civil, no sentido não apenas de prevenir medidas ilegais, mas também de informar esses processos com os insumos necessários à sua condução de forma legítima e eficiente (Bioni, Zanatta, Monteiro e Rielli, 2020; Doneda 2020; Edwards, 2020).

Ao contrário do caso da Europa, onde diversos países já possuem ambiente institucional de proteção de dados consolidado há décadas com leis gerais e autoridades de proteção de dados (Bennett & Raab, 2018), no Brasil esses debates foram agravados pela fragilidade institucional do quadro de proteção de dados no país quando a os primeiros casos de transmissão comunitária foram confirmados. Conforme exposto anteriormente, tanto a vigência pendente da LGPD, quanto a ausência de iniciativa do governo para criação de uma autoridade nacional de proteção de dados, tornavam os cidadãos ainda mais expostos diante da crise sanitária cujo combate passava pelo uso massivo da coleta e tratamento de dados. Nesse momento, as preocupações passavam tanto pela possibilidade de adoção de medidas de vigilância potencialmente irreversíveis (Evangelista e Firmino,

2020), quanto pelo uso da pandemia como subterfúgio para mais adiamentos da vigência da LGPD (Keller e Pereira, 2020).

Apesar disso, não se verifica um quadro institucional ainda mais enfraquecido de proteção de dados. Pelo contrário; é possível afirmar que, a partir da movimentação da academia e da sociedade civil – e notadamente, do resultado da judicialização da matéria na corte constitucional por partidos políticos e pelo Conselho Federal da OAB – esse quadro se encontra, hoje, fortalecido. Além da decisão do STF explorada na seção anterior, recentemente o Senado Federal rejeitou o adiamento da vigência da LGPD ao votar a MP 959/2020, de forma que a primeira lei nacional de proteção de dados entrou em vigor no dia 18 de setembro de 2020, após ser sanção pelo presidente da república. No dia seguinte à decisão do Senado, foi publicado o Decreto 10.474/2020, que aprova a estrutura regimental e o quadro de cargos da ANPD. Ainda que o formato atual da autoridade, ligada diretamente à Presidência da República, seja questionável (Keller, 2019, p. 243-245), espera-se que esse seja um pontapé inicial para a composição e própria operação da LGPD.

É certo que esse quadro também pode ser atribuído a outros fatores. A discussão sobre proteção de dados no Brasil e a gestão de uma lei geral levaram anos,[19] e a aprovação da lei tinha de fato importância política previamente à pandemia (Mendes e Doneda, 2018). Além disso, durante a pandemia de COVID- 19 foi também insuflado, no Congresso Nacional, o debate sobre combate à desinformação (Galf, 2020), que se relaciona de forma indissociável com a proteção de dados (Bennet e Lyon, 2019). Contudo, é patente que o "contramovimento" (Hildebrandt, 2020) liderado diante dos riscos que a pandemia de COVID- 19 representava para os direitos à privacidade e proteção de dados teve um papel determinante nas decisões tomadas em relação à matéria das diferentes instâncias de estado.

De fato, esse efeito também pode ser observado em outras experiências nacionais. Conforme descrito na primeira parte do texto, governos de outros países também adaptaram ou mudaram suas abordagens iniciais sobre uso de tecnologia para combate à COVID- 19 após reações da sociedade civil e da academia. Veja-se, por exemplo, os já descritos casos de Cingapura e alguns países da União Europeia, que optaram pela solução descentralizada oferecida por Apple e Google após reações negativas às suas primeiras medidas (item 2.1, *supra*); ou o caso

[19] Veja, nesse sentido, a série de entrevistas do projeto "Memória da LGPD", que é um documentário de cinco capítulos e mais de cento e cinquenta microvídeos sobre o processo de articulação da lei de proteção de dados no Brasil. Disponível em: https://observatorioprivacidade.com.br/memorias/. Acesso em: 23 set. 2020.

da Noruega, onde uma reação semelhante foi gerada por um relatório da Anistia Internacional (item 2.2.1, *supra*).

No Brasil, é possível afirmar que esse contramovimento atingiu seu ápice no sucesso da judicialização da MP 954/2020 no Supremo Tribunal Federal. Junto com as demais determinações da Corte, o reconhecimento do status constitucional da proteção de dados configura uma conquista institucional fundamental, tanto pela força formal do precedente, quanto pelo seu simbolismo. E até pela mensagem que deixa registrada para os atores brasileiros sobre o tratamento de dados durante uma pandemia: a de que o Tribunal reconhece e privilegia a centralidade da proteção de dados nas sociedades contemporâneas, bem como a sua relação com o cumprimento de garantias constitucionais individuais e coletivas. É interessante notar que, no caso em questão, apesar da matéria de fato ter uma relação de causalidade com a pandemia, não se tratava, exatamente, do uso de uma das tecnologias descritas na seção 2. Um lembrete de que a proteção de dados não é uma preocupação exclusiva da digitalização (como nos mostra a história da sua evolução) e uma bela ilustração da sua amplitude (e, por conseguinte, da importância de sua proteção).

Diante do inegável avanço no quadro institucional da proteção de dados no Brasil, importa registrar os desafios que permanecem à frente. Em primeiro lugar, como mencionado anteriormente, o formato atual da ANPD, ligada diretamente à Presidência da República compromete, em muito, a independência necessária aos órgãos executores de política pública (Keller, 2019, p. 243-245). Em segundo lugar, cabe observar que tramita no Congresso Nacional a PEC 17/19, cujo objeto é a incorporação de um direito fundamental à proteção de dados pessoais ao catálogo de direitos e garantias da Constituição Federal. Apesar da decisão do STF ter reconhecido seu status de norma constitucional, há quem entenda que a previsão em texto constitucional daria ainda maior institucionalidade a esse direito (Bioni & Mota, 2020). Conforme apontado por Ingo Sarlet, a positivação formal da proteção de dados na Constituição carregaria consigo "carga positiva adicional, ou seja, agrega (ou ao menos, assim deveria) valor positivo substancial em relação ao atual estado da arte no Brasil" (2020). Dentre as vantagens da inclusão formal na Constituição, o autor enumera: (i) a segurança da proteção de dados como direito fundamental autônomo, com âmbito de proteção próprio; e (ii) atribuição de modo inquestionável do pleno regime jurídico-constitucional relativo ao seu perfil de direito fundamental em sentido material e formal (status normativo superior em relação a todo o restante do ordenamento jurídico nacional, aplicabilidade dos limites conferidos às cláusulas pétreas e aplicabilidade direta, vinculando atores públicos e privados).

Em terceiro lugar, a movimentação do Senado Federal de manter a vigência da LGPD pode reforçar a constitucionalização da proteção de dados pessoais. Se,

nas palavras do Ministro Gilmar Mendes, é imperativo garantir "mecanismos institucionais de salvaguarda traduzidos em normas de organização e procedimento (Recht auf Organisation und Verfahren)", pode surgir a tese de que a inação do governo federal em criar a Autoridade Nacional de Proteção de Dados Pessoais configura omissão constitucional. A aprovação do Decreto n. 10.474/2020, que aprova a estrutura regimental da Autoridade Nacional de Proteção de Dados, pode ser compreendida como uma tentativa do governo de mitigar os riscos de um mandado de injunção coletivo, nos termos da Lei 13.300/2016. Nos termos do art. 2º da referida lei, "conceder-se-á mandado de injunção sempre que a falta total ou parcial de norma regulamentadora torne inviável o exercício dos direitos e liberdades constitucionais e das prerrogativas inerentes à nacionalidade, à soberania e à cidadania". Com a decisão do STF e a ausência de Decreto, abrir-se-ia a possibilidade de argumentar que a omissão legislativa estaria afetando o gozo de direitos fundamentais, justamente pela ausência de mecanismos institucionais de salvaguardas capazes de dar concretude a esse direito.

6 Conclusão

A pandemia da COVID- 19 abriu espaço para um amplo debate sobre o papel das novas tecnologias e do uso de dados pessoais no combate ao vírus. Como demonstrado, esse debate foi fomentado pela implementação de projetos e parcerias público-privadas que usavam, principalmente, índices de aglomeração, mapas de calor e técnicas de rastreamento digital. Ao redor do globo, essas iniciativas geraram preocupações e um amplo debate sobre a sua legitimidade, principalmente em relação aos riscos para os direitos à privacidade e proteção de dados das populações.

No Brasil, as principais iniciativas nesse sentido foram uma ferramenta de geolocalização para geração de mapas de calor desenvolvida por empresa privada e o SIMI-SP, que envolveu empresas de telecomunicações. As empresas de telecomunicações também foram alvo de grande polêmica com a Medida Provisória que pretendeu compartilhar dados de seus consumidores com o IBGE, permitindo a realização de pesquisas estatísticas pelo telefone. As contestações da OAB e dos partidos políticos permitiram ao Supremo Tribunal Federal se posicionar sobre o assunto, criando uma janela de oportunidade para a afirmação da proteção de dados pessoais como direitos fundamentais.

É cedo para realizar um balanço completo do impacto da COVID- 19 para a vigilância no Brasil. Apesar dos diversos receios e polêmicas com relação ao uso de dados pessoais e o compartilhamento de dados entre empresas privadas e

governo, o olhar atento da comunidade jurídica e os contra movimentos gerados por organizações de defesa de direitos, nos dizeres de Mireille Hildebrandt, impactaram na constitucionalização da proteção de dados e trouxeram um saldo positivo para a agenda de proteção de dados pessoais. Os projetos futuros de uso de tecnologias no combate à COVID- 19 – sejam eles mapas de calor por GPS, apps de rastreamento de contatos por Bluetooth ou outras técnicas de análise massiva de dados obtidos de celulares ou redes sociais – precisarão passar pelo crivo da Lei Geral de Proteção de Dados e pela análise interpretativa da comunidade jurídica, inspirada por novos precedentes e pela decisão recente do STF. Assim como a pandemia, as tensões jurídicas estão longe de acabar.

Abstract: This article presents the main findings of the research project "Os dados e o vírus" (which followed and documented the use of information and communication technologies – ICTs to combat the Covid-19 pandemic). Since they fostered the debate on the legitimacy of these technologies, the article also offers an analysis, focused on the Brazilian case, of how the country's data protection institutional framework was affected. We describe the main technologies based on data collection and treatment used at a global level, as well as the main cases of adoption in Brazil. We also address the judicial tensions caused by these uses and by attempts to share personal data in the context of Covid-19 (Ação Popular nº 1019257-34.2020.8.26.0053 and ADI 6387). Next, we analyzed the impacts of these debates and lawsuits on the country's data protection foundations. Among the conclusions we reached, the strengthening of this institutional framework stands out, contradicting initial concerns that the adoption of the technologies described would favor its weakening.

Keywords: data protection; contact tracing; surveillance; COVID- 19.

Referências

ALMEIDA, Bethania de Araujo *et al*. Preservação da privacidade no enfrentamento da COVID-19: dados pessoais e a pandemia global. Ciênc. saúde coletiva, Rio de Janeiro, v. 25, supl. 1, p. 2487-2492, jun. 2020. Disponível em: http://www.scielo.br/scielo.php?script=sci_arttext&pid=S1413-81232020006702487&lng=pt&nrm=iso

ALTUWAIYAN, Thamer; HADIAN, Mohammad; LIANG, Xiaohui. EPIC: efficient privacy-preserving contact tracing for infection detection. *In*: 2018 *IEEE International Conference on Communications (ICC)*. IEEE, 2018. p. 1-6.

AMARAL, Bruno do. *Coronavírus: TIM e Prefeitura do Rio assinam acordo para coletar dados de deslocamento*, Teletime, 23 mar. 2020. Disponível em:: https://teletime.com.br/23/03/2020/coronavirus-tim-e-prefeitura-do-rio-assinam-acordo-para-coletar-dados-de-deslocamento/. Acesso em: 23 set. 2020.

AMNESTY INTERNATIONAL. Bahrain, Kuwait and Norway contact tracing apps a danger for privacy. Disponível em:: https://www.amnesty.org/en/latest/news/2020/06/bahrain-kuwait-norway-contact-tracing-apps-danger-for-privacy/. Acesso em: 30 jul. 2020.

ANDRÉ, Natália. *Governo diz que vai usar dados de celulares para monitorar aglomerações*, CNN, 27 mar. 2020. Disponível em: https://www.cnnbrasil.com.br/tecnologia/2020/03/27/ministerio-da-ciencia-vai-monitorar-celulares-para-conter-aglomeracoes. Acesso em: 23 set. 2020.

BARILLI, Fabrício. *Coronavírus: um intensificador do estado de vigilância*, in Data Privacy (org.), *Os dados e o virus: pandemia, proteção de dados e democracia*, São Paulo, 2020. Disponível em: https://www.dataprivacybr.org/wp-content/uploads/2020/09/eBook_selecoes_osdados_eo_virus.pdf. Acesso em: 23 set. 2020.

BENNET, Colin e LYON, David. Data driven elections: implications and challenges for data driven societies. *Internet Policy Review,* 8(4). DOI: 10.14763/2019.4.1433.

BIONI, Bruno; ALVES, Fabrício Mota. A importância da PEC de proteção de dados mesmo após o histórico julgamento do STF. *JOTA Info*. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/a-importancia-da-pec-de-protecao-de-dados-mesmo-apos-o-historico-julgamento-do-stf-16062020. Acesso em: 30 set. 2020.

BIONI, Bruno; BIONI, Ricardo. *Proteção de dados pessoais*: a função e os limites do consentimento. Rio de Janeiro: Grupo Editorial Nacional, 2019.

BIONI, Bruno; MARTINS, Pedro. Devido processo informacional: um salto teórico-dogmático necessário? *JOTA*, 15 julho 2020. Disponível em: www.jota.info/opiniao-e-analise/artigos/devido-processo-informacional-um-salto-teorico-dogmatico-necessario-15072020

BIONI, Bruno; MONTEIRO, Renato Leite. A Landmark Ruling in Brazil: Paving the Way for Considering Data Protection as an Autonomous Fundamental Right, *Future of Privacy Forum*, June 9, 2020. Disponível em: https://fpf.org/2020/06/09/a-landmark-ruling-in-brazil-paving-the-way-for-considering-data-protection-as-an-autonomous-fundamental-right/

BIONI, Bruno; ZANATTA, Rafael; MONTEIRO, Renato; RIELLI, Mariana. *Privacidade e pandemia: recomendações para o uso legítimo de dados no combate à COVID-19*. São Paulo: Data Privacy Brasil, 2020.

BIONI, Bruno; ZANATTA, Rafael. Proteção de dados faz parte da vacina contra COVID-19. *JOTA*, 04 maio. 2020. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/protecao-de-dados-faz-parte-da-vacina-contra-covid-19-04052020

BYFORD, Sam. Japan rolls out Microsoft-developed COVID-19 contact tracing app. *The Verge*. Disponível em: https://www.theverge.com/2020/6/19/21296603/japan-covid-19-contact-tracking-app-cocoa-released. Acesso em: 30 jul. 2020.

CHEN, Chi-Mai; JYAN, Hong-Wei; CHIEN, Shih-Chieh *et al*. Containing COVID-19 Among 627,386 Persons in Contact With the Diamond Princess Cruise Ship Passengers Who Disembarked in Taiwan: Big Data Analytics. *Journal of Medical Internet Research*, v. 22, n. 5, p. e19540, 2020.

CHO, Hyunghoon; IPPOLITO, Daphne; YU, Yun William. Contact tracing mobile apps for COVID-19: Privacy considerations and related trade-offs. *arXiv preprint arXiv*:2003.11511, 2020.

DONEDA, Danilo. *A proteção de dados em tempos de coronavírus*, Jota, 25 mar. 2020. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/a-protecao-de-dados-em-tempos-de-coronavirus-25032020. Acesso em: 23 set. 2020.

EDPS. *TechDispatch #1/2020*: Contact Tracing with Mobile Applications | European Data Protection Supervisor. Disponível em: https://edps.europa.eu/data-protection/our-work/publications/techdispatch/techdispatch-12020-contact-tracing-mobile_en. Acesso em: 30 jul. 2020.

EDWARDS, Lilian. Apps, politics, and power: protecting rights with legal and software code. *In*: TAYLOR, Linnet; SHARMA, Gargi; MARTIN, Aaron e JAMESON, Shazade. *Data Justice and COVID-19: Global Perspectives*, Meatspace Press: London, 2020.

ENDO, Patricia Takako *et al*. # StayHome: Monitoring and benchmarking social isolation trends in Caruaru and the Região Metropolitana do Recife during the COVID-19 pandemic. Revista da Sociedade Brasileira de Medicina Tropical, v. 53, 2020.

ELKIN-KOREN, Niva. Judicial review of digital tracking measures in corona outbreak. *Internet Policy Review*, 20 mar. 2020. Disponível em: https://policyreview.info/articles/news/judicial-review-digital-tracking-measures-coronavirus-outbreak/1451. Acesso em: 23 set. 2020.

EVANGELISTA, Rafael e FIRMINO, Rodrigo. Brazil – Modes of pandemic existence: territory, inequality and technology. *In*: TAYLOR, Linnet; SHARMA, Gargi; MARTIN, Aaron e JAMESON, Shazade. *Data Justice and COVID-19: Global Perspectives*, Meatspace Press: London, 2020.

FARRAHI, Katayoun; EMONET, Remi; CEBRIAN, Manuel. Epidemic contact tracing via communication traces. *PloS one*, v. 9, n. 5, p. e95133, 2014.

FERNANDES, Elora Raad. Resenha à obra LGPD e o novo marco normativo no Brasil, de Mulholland, Caitlin (Org.). *Revista Brasileira de Direito Civil – RBDCivil*, Belo Horizonte, v. 24, p. 263-266, abr./jun. 2020.

FERRETTI, Luca; WYMANT, Chris; KENDALL, Michelle *et al*. Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing. *Science*, v. 368, n. 6491, p. eabb6936, 2020.

FIGUEIREDO, A. M. *et al*. Impact of lockdown on COVID-19 incidence and mortality in China: an interrupted time series study. *Bull World Health Organ*, 2020.

Gill, L., REDEKER, Dennis and GASSER, Urs. 2015. "Towards Digital Constitutionalism? Mapping Attempts to Craft an Internet Bill of Rights." *Berkman Klein Center for Internet & Society Research Publication* No. 2015-15.

G1 PE. Recife rastreia 700 mil celulares para monitorar isolamento social e direcionar ações contra coronavírus*, G1*, 24 mar. 2020. Disponível em: https://g1.globo.com/pe/pernambuco/noticia/2020/03/24/recife-rastreia-700-mil-celulares-para-monitorar-isolamento-social-e-direcionar-acoes-contra-coronavirus.ghtml. Acesso em: 23 set. 2020.

GALF, Renata. Lei das *fake news* pode ser útil, mas especialistas pedem calma no Congresso. *Folha de São Paulo*, 25 ago. 2020. Disponível em: https://www1.folha.uol.com.br/poder/2020/08/lei-das-fake-news-pode-ser-util-mas-especialistas-pedem-cautela-ao-congresso.shtml. Acesso em: 23 set. 2020.

GOMES, Helton. Cliente da TIM aciona Justiça e tem celular excluído do monitoramento de SP. *UOL*. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2020/04/17/cliente-da-tim-consegue-na-justica-sair-do-monitoramento-de-celular-em-sp.htm. Acesso em: 30 jul. 2020.

GOMES, Juliana Cesario Alvim. Nas encruzilhadas: limites e possibilidades do uso do litígio estratégico para o avanço dos direitos humanos e para a transformação social. *Rev. Direito Práxis*, Rio de Janeiro, v. 10, n. 1, p. 389-423, 2019.

GLOBAL PRIVACY ASSEMBLY. COVID-19 *Resources Library*. Disponível em: https://globalprivacyassembly.org/covid19/covid19-resources/

GUZZETTA, Giorgio *et al*. The impact of a nation-wide lockdown on COVID-19 transmissibility in Italy. *arXiv preprint* arXiv:2004.12338, 2020.

HAN, Byung Chul. O coronavírus de hoje e o mundo de amanhã, *El País*, 22/03/2020. Disponível em: https://brasil.elpais.com/ideas/2020-03-22/o-coronavirus-de-hoje-e-o-mundo-de-amanha-segundo-o-filosofo-byung-chul-han.html

HAYWARD, Tim *et al*. *Constitutional environmental rights*. Oxford University Press, 2005.

HILDEBRANDT, Mireille. Countermovements to Reinstate Countervailing Powers (reviewing Julie E. Cohen, Between Truth and Power: The Legal Constructions of Informational Capitalism (2019), *JOTWELL*, July, 2020. Disponível em: https://cyber.jotwell.com/countermovements-to-reinstate-countervailing-powers/.

IPT. Perguntas sobre isolamento social, *IPT*, 03/06/2020. Disponível em: https://www.ipt.br/noticia/1623-_perguntas_sobre_isolamento_social.htm

JEFFORDS, Chris; GELLERS, Joshua C. Constitutionalizing Environmental Rights: A Practical Guide. *Journal of Human Rights Practice*, v. 9, n. 1, p. 136-145, 2017.

LEAL, Fernando. O Supremo e a pandemia: é preciso uma jurisprudência da crise? *Jota*, 01 abr. 2020. Disponível em: https://www.jota.info/stf/supra/stf-pandemia-crise-jurisprudencia-01042020. Acesso em: 23 set. 2020.

KELLER, Clara Iglesias. *Regulação nacional de serviços na Internet*: exceção, legitimidade e o papel do Estado. Lumen Juris: Rio de Janeiro, 2019.

KELLER, Clara Iglesias; PEREIRA, Jane Reis Gonçalves. Data protection in times of Covid-19: the risks for surveillance in Brazil, *Internet Policy Review*, 01 abr. 2020. Disponível em: https://policyreview.info/articles/news/data-protection-times-covid-19-risks-surveillance-brazil/1462. Acesso em: 23 set. 2020.

MEDAUAR, Odete. *Direito Administrativo Moderno*. 21ª ed. Belo Horizonte: Fórum, 2018.

MEDEIROS, Henrique. *MP do Distrito Federal arquiva inquérito contra In Loco, MobileTime*, 20/02/2020. Disponível em: https://www.mobiletime.com.br/noticias/20/02/2020/mp-do-distrito-federal-arquiva-inquerito-contra-a-in-loco/

MENDES, Laura Schertel. *Transparência e privacidade*: violação e proteção da informação pessoal na sociedade de consumo. 2008. 156 f. Dissertação (Mestrado em Direito) – Universidade de Brasília, Brasília, 2008.

MENDES, Laura Schertel. Decisão histórica do STF reconhece direito fundamental à proteção de dados pessoais, *Jota*, 10/05/2020. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/decisao-historica-do-stf-reconhece-direito-fundamental-a-protecao-de-dados-pessoais-10052020. Acesso em: 29 set. 2020.

MENDES, Laura Schertel; DONEDA, Danilo. Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados. *Revista dos Tribunais Online*, vol. 120, 2018, p. 469-482.

MENDES, Laura Schertel; FONSECA, Gabriel. STF reconhece direito fundamental à proteção de dados: comentários sobre o referendo da medida cautelar nas ADIs 6387, 6388, 6389, 6390 e 6393, *Revista de Direito do Consumidor*, v. 130, jul/ago, 2020, p. 471-478

NASCIMENTO, Luciano. Brasil acumula 141.406 mortes pelo novo coronavirus, *Agência Brasil*, 26 set. 2020. Disponível em: https://agenciabrasil.ebc.com.br/saude/noticia/2020-09/brasil-acumula-141406-mortes-pelo-novo-coronavirus. Acesso em: 26 set. 2020.

NICAS, Jack; WAKABAYASHI, Daisuke. Apple and Google Team Up to 'Contact Trace' the Coronavirus. *The New York Times*, 2020. Disponível em: https://www.nytimes.com/2020/04/10/technology/apple-google-coronavirus-contact-tracing.html. Acesso em: 30 jul. 2020.

NOGUEIRA, Luiz. "Covid-19: Vivo e governo de SP vão usar dados para rastrear doença". *Olhar Digital*, 02 abr. 2020. Disponível em: https://olhardigital.com.br/coronavirus/noticia/covid-19-governo-de-sp-e-vivo-usarao-dados-para-rastrear-doenca/98900. Acesso em: 23 set. 2020.

PALHARES, Gabriela *et al*. A privacidade em tempos de pandemia e a escada de monitoramento e rastreio. *Estudos Avançados*, v. 34, n. 99, p. 175-190, 2020. Disponível em: https://www.scielo.br/scielo.php?pid=S0103-40142020000200175&script=sci_arttext&tlng=pt

POLLO, Luiza *et al*. Tudo o que você precisa saber sobre as tecnologias de rastreamento utilizadas no combate à Covida-19. *Observatório da Privacidade e da Proteção de Dados Pessoais*, 21 de setembro de 2020. Disponível em: https://observatorioprivacidade.com.br/2020/09/21/tudo-o-que-voce-precisa-saber-sobre-as-tecnologias-de-rastreamento-utilizadas-no-combate-a-covid-19/

PAN, Xiao-Ben. Application of personal-oriented digital technology in preventing transmission of COVID-19, China. *Irish Journal of Medical Science* (1971-), p. 1-2, 2020.

RASKAR, Ramesh; SCHUNEMANN, Isabel; BARBAR, Rachel *et al*. Apps Gone Rogue: Maintaining Personal Privacy in an Epidemic. *arXiv:2003.08567* [cs], 2020. Disponível em: http://arxiv.org/abs/2003.08567. Acesso em: 30 jul. 2020.

REQUIÃO, Maurício. Covid-19 e a proteção de dados pessoais: o antes, o agora e o depois. *Conjur*, 5 de abril, 2020. Disponível em: https://www.conjur.com.br/2020-abr-05/direito-civil-atual-covid-19-protecao-dados-pessoais-antes-agora-depois Acesso em: 29 set. 2020.

SARLET, Ingo Wolfgang. Precisamos de um direito fundamental à proteção de dados no texto da CF? *Conjur*, 04 set. 2020. Disponível em: https://www.conjur.com.br/2020-set-04/direitos-fundamentais-precisamos-previsao-direito-fundamental-protecao-dados-cf. Acesso em 23 set. 2020.

SINGER, Natasha. *Google Coronavirus Apps Give it Way to Access Location Data*. Disponível em: https://www.nytimes.com/2020/07/20/technology/google-covid-tracker-app.html. Acesso em: 30 jul. 2020.

THOMPSON, Stuart; WARZEL, Charlie. Twelve Million Phones, One Dataset, Zero Privacy. The Privacy Project. *The New York Times*, 19/12/2019. Disponível em: https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html

VAUDENAY, Serge. *Centralized or decentralized*? the contact tracing dilemma, EPFL, Lausanne, 2020. Disponível em: https://infoscience.epfl.ch/record/277809?&ln=en

VAN BAVEL, Jay J. *et al*. Using social and behavioural science to support COVID-19 pandemic response. *Nature Human Behaviour*, p. 1-12, 2020.

VAN KOLFSCHOOTEN, Hannah; DE RUIJTER, Anniek. COVID-19 and privacy in the European Union: A legal perspective on contact tracing. *Contemporary Security Policy*, p. 1-14, 2020.

VIPIANA, Tabata. Doria é questionado na Justiça por monitoramento de celulares no estado. *Conjur*, 14/04/2020. Disponível em: https://www.conjur.com.br/2020-abr-14/doria-questionado-justica-monitoramento-celulares

WHO, CDC. Implementation and management of contact tracing for Ebola virus disease. WHO/EVD/Guidance/Contact/15.1. Setembro de 2015. Disponível em: https://apps.who.int/iris/bitstream/handle/10665/185258/WHO_EVD_Guidance_Contact_15.1_eng.pdf;jsessionid=B7FE1CBC9DE7D71535BD77B6D14DB9D0?sequence=1. Acesso em: 30 jul. 2020.

WRIGHT, Susie. *Contact tracing apps for COVID-19*. 2020. Disponível em: https://post.parliament.uk/analysis/contact-tracing-apps-for-covid-19/,

Informação bibliográfica deste texto, conforme a NBR 6023:2018 da Associação Brasileira de Normas Técnicas (ABNT):

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

Recebido em: 31.07.2020
Pareceres: 30.08.2020, 23.08.2020
Aprovado em: 12.09.2020