ARTIGO

Privacidade, proteção de dados pessoais e crises epidemiológicas: racionalidades e lições da pandemia

Jacqueline de Souza Abreu
jacqueabreu@gmail.com

Doutoranda em Direito na Universidade de São Paulo e advogada. Mestra em direito pela UC Berkeley e pela LMU München.

V. 2 / N. 1 / JUNHO DE 2021
PÁGINAS 5 A 26

Privacidade, proteção de dados pessoais e crises epidemiológicas: racionalidades e lições da pandemia

Palavras-chave
privacidade
proteção de dados
vigilância epidemiológica
controle sanitário

Resumo
O presente artigo explora o escopo dos direitos à privacidade e à proteção de dados pessoais no contexto de crises epidemiológicas e as lições que a pandemia da COVID-19 deixa para a área no Brasil. Para tanto, o trabalho retoma discussões sobre inviolabilidade do domicílio no contexto de estratégias de combate à dengue. A seguir, apresenta as discussões sobre uso de dados que ganharam repercussão no Brasil durante a pandemia: o compartilhamento de dados de empresas com o IBGE e a implementação do SIMI pelo Governo de São Paulo. A seguir, discute como ilustram as distintas intencionalidades do direito à privacidade e da proteção de dados. Por fim, expande as considerações sobre proteção de dados pessoais no contexto de vigilância e controle epidemiológico para extrair lições sobre (i) o encontro entre lógicas de precaução dessa área do direito com a do direito sanitário, (ii) a relevância do princípio da legalidade e (iii) o respeito à divisão informacional de poderes.

Privacy, data protection, and epidemiological crises: rationalities and lessons from the pandemic

Key-words
privacy
data protection
epidemiological surveillance
public health

Abstract
This article explores the scope of the rights to privacy and data protection in the context of epidemiological crises and the lessons that the COVID-19 pandemic leaves for the area in Brazil. To this end, the work resumes discussions about the inviolability of the home in the context of strategies to combat dengue. Next, it presents the discussions on the use of data that gained repercussion in Brazil during the pandemic: the sharing of telcos data with the Brazilian Institute of Geography and Statistics (IBGE) and the implementation of the Smart Monitoring System (SIMI) by the Government of São Paulo. Then it discusses how they illustrate the different purposes of the right to privacy and data protection. Finally, the paper expands the considerations about data protection in the context of epidemiological control and surveillance to draw lessons on (i) the encounter between the precautionary logic of this area of law with that of health law, (ii) the relevance of the legality principle and (iii) the respect for the informational division of powers.

1. Introdução

O presente artigo[1] pretende explorar como a compreensão jurídica dos contornos dos direitos à privacidade e à proteção de dados pessoais se dá em meio a crises epidemiológicas – e, assim, como esses direitos operam frente a ações estatais motivadas pela proteção da saúde pública. De forma específica, pretende-se mostrar – a partir de pesquisa bibliográfica e documental e análise de exemplos práticos – como a discussão atual da pandemia do COVID-19 salientou a dimensão *procedimental* do direito à proteção de dados pessoais – voltada ao resguardo de regras, princípios, métodos, salvaguardas contra riscos de danos e abusos no uso de dados pessoais. Esta dimensão também existe em nossa compreensão do direito à privacidade e de como protege-lo, mas ganhou protagonismo com o direito à proteção de dados e deixou lições sobre a natureza e o modo de funcionamento desse direito que devem ser consolidados na ainda breve história da área no Brasil.

Para tanto, inicia-se o trabalho retomando discussões sobre inviolabilidade do domicílio no contexto de estratégias de combate à dengue (Parte 1). A seguir, apresentam-se as discussões sobre uso de dados que ganharam repercussão no Brasil durante a pandemia: o compartilhamento de dados de empresas com o IBGE e a implementação do SIMI pelo Governo de São Paulo (Parte 2). A seguir, discute-se como esses casos ilustram as distintas intencionalidades do direito à privacidade e da proteção de dados (Parte 3). Por fim, expandem-se as considerações sobre proteção de dados pessoais no contexto de vigilância e controle epidemiológico para extrair lições sobre (i) o encontro entre lógicas de precaução dessa área do direito com a do direito sanitário, (ii) a relevância do princípio da legalidade e (iii) a observância da divisão informacional de poderes (Parte 4).

2. O combate à dengue e a inviolabilidade do domicílio

Privacidade é um direito fundamental cujo sentido e alcance dependem do contexto de aplicação. Ninguém caracteriza o ingresso, mediante convite, de um amigo ou vizinho à própria casa como uma violação da privacidade do lar – da inviolabilidade do domicílio. Não é mesmo violação: nesse caso, se decidiu dispor sobre a privacidade para estendê-la ao amigo ou vizinho – inclusive como demonstração da relação íntima ou de confiança entre eles. Já o ingresso por terceiro não-autorizado no lar de alguém é crime (art. 150, Código Penal).

Quando uma autoridade policial investigando crime quer ingressar em alguma residência, as circunstâncias começam a mudar. Também aqui, entende-se que, se o responsável autoriza espontaneamente o ingresso no lar, não se pode falar em violação. Caso não haja autorização, um mandado judicial de busca e apreensão baseado em indícios de que dentro de uma casa há elementos de prova que podem auxiliar a elucidação de um crime pode autorizar o ingresso, superando a vontade do titular. Também a situação de flagrante delito, desde que amparada em fundadas suspeitas de que ocorre delito dentro da casa, é capaz de justificar excepcionalmente o ingresso.[2]

O combate à dengue – anos atrás – provocou operadores do direito a terem de lidar com uma nova discussão sobre o alcance da inviolabilidade do domicílio resguardada pela Constituição Federal de 1988 (art. 5º, XI). Agentes de saúde encarregados de realizar o controle vetorial da doença, visitando casa a casa à procura de focos do *aedes aegypti*, podem contar com a boa vontade dos proprietários para seu ingresso em residências. Mas o que fazer com aqueles que não estão em casa ou

que se recusam a autorizar o ingresso dos agentes? Também aqui é possível imaginar que a existência de um mandado judicial ou até mesmo uma situação de flagrante delito, baseada em fundadas suspeitas de que o local é foco da doença, poderia autorizar o ingresso contra ou sem manifestação de vontade.

Mas seria possível dispensar essas exigências? Isto é, dispensar o mandado judicial e a verificação concreta de situação de flagrância? Em 2002, uma edição especial da *Revista de Direito Sanitário* se dedicou ao assunto – sob a perspectiva de que a situação colocava exigências do estado de proteção à saúde pública, de um lado, e o direito à inviolabilidade do domicílio, de outro, frente a um expressivo salto de casos da doença ocorrido àquela época.

Uma das observações mais valiosas de um dos debatedores foi a de que o ingresso forçado no contexto de programa de vigilância epidemiológica[3] "é claramente geral, envolvendo todos os ambientes de uma dada região", sem "cunho de pessoalidade" nem potencial de gerar um "subproduto negativo" para o particular (Sundfeld, 2002, p. 104). Isso seria profundamente distinto das hipóteses de ingresso para fins policiais em investigações – em que a medida é específica, deve ser baseada em causa legítima e suficiente para que não constitua abuso, e tem repercussões penais. De fato, no contexto epidemiológico, sequer há *busca* sobre o domicílio que abranja aspectos íntimos, apenas ingresso voltado a áreas focais da doença. Não é possível dizer que o Estado está intervindo na soberania de alguém sobre a disposição da sua identidade e intimidade, muito embora o faça sobre a sua propriedade. São contextos, portanto, diferentes – e que mereceriam tratamento jurídico diferente. O direito à privacidade do lar não inclui um direito de impedir profissionais da saúde de combaterem focos de mosquito que transmite doença contagiosa.

Após anos de controvérsia[4] sobre a necessidade ou não de uma previsão legal específica, a questão foi tratada em lei federal. A Lei nº 13.301/16 previu o "*ingresso forçado em imóveis públicos e particulares, no caso de situação de abandono, ausência ou recusa de pessoa que possa permitir o acesso de agente público, regularmente designado e identificado, quando se mostre essencial para a contenção das doenças*" causadas pelo vírus da dengue, do vírus chikungunya e do vírus da zika (art. 1º, §1º, IV).

Para tanto, estabeleceu as seguintes premissas e condições: (i) definições precisas das situações que caracterizam "imóvel em situação de abandono", "ausência" e "recusa" (art. 1º, §2º). Por exemplo, a ausência somente poderia ser caracterizada na "impossibilidade de localização de pessoa que possa permitir o acesso ao imóvel na hipótese de duas visitas devidamente comunicadas, em dias e períodos alternados, dentro do intervalo de dez dias" (art. 1º, §2º, II)".

Também prevê que "o ingresso forçado será realizado buscando a preservação da integridade do imóvel e das condições de segurança em que foi encontrado" (art. 2º), "[s]empre que se mostrar necessário, o agente público competente poderá requerer auxílio à autoridade policial ou à Guarda Municipal" (art. 3º, §1º) e "nos casos de ingresso forçado em imóveis públicos e particulares, o agente público competente emitirá relatório circunstanciado no local" (art. 3º). No relatório circunstanciado devem constar (art. 3º, § 2º): I - as condições em que foi encontrado o imóvel; II - as medidas sanitárias adotadas para o controle do vetor e da eliminação de criadouros do mosquito transmissor do vírus da dengue, do vírus chikungunya e do vírus da zika; III - as recomendações a serem observadas pelo responsável; e IV - as medidas adotadas para restabelecer a segurança do imóvel. Por fim, o art. 4º permite que a medida seja aplicada excepcionalmente ao combate a outras doenças que importem em grave risco ou ameaça à saúde pública, condicionada à declaração de Emergência em Saúde Pública de Importância Nacional - ESPIN.

Como se vê, a lei cria uma autorização excepcional ao ingresso em domicílio para implementação de medida de saúde pública de eficácia inequívoca e sem danos colaterais a liberdades. Ao fazer isso, estabelece de forma específica o procedimento a ser observado para garantir a sua integridade, nos estritos termos da finalidade de combate à doença. A lei foi objeto de questionamento no Supremo Tribunal Federal por outros dispositivos[5], mas não por incorrer em uma violação à proteção constitucional da inviolabilidade do domicílio – o que sugere que a forma de ajuste proposta na lei correspondeu às expectativas normativas acerca do equilíbrio entre o direito à inviolabilidade do domicílio e as prerrogativas do poder de polícia atinentes à proteção da saúde pública, estabelecendo salvaguardas adequadas contra abusos.

3. As discussões de proteção de dados trazidas pela COVID-19

A pandemia da COVID-19 fez surgir novas discussões sobre os limites do interesse público no controle e monitoramento epidemiológico em liberdades individuais no contexto de propostas e iniciativas que envolviam usos de dados pessoais.

No Brasil, duas discussões ganharam bastante repercussão. Primeiro, a imposição, por medida provisória (MP nº 954 de 17.04.2020), de uma obrigação de empresas de telecomunicações compartilharem bases de dados de nomes, telefone e endereço com o Instituto Brasileiro de Geografia e Estatística (IBGE) para execução de pesquisas por telefone durante a pandemia. A medida em si não estava imediatamente ligada ao combate à doença, mas à necessidade de dar continuidade a pesquisas anuais que, inclusive, pudessem medir o impacto da pandemia. Segundo, a celebração de acordos entre governos, principalmente estaduais, e empresas de telecomunicações ou empresas de inteligência de marketing em geolocalização, para compartilhamento de dados agregados de geolocalização, que informem taxas de isolamento domiciliar e mapas de calor (para identificação de eventuais pontos de aglomeração).

Para registro, essas não foram a únicas discussões. Cogitou-se pesquisa sobre sintomas por telefone – tendo o Ministério da Saúde inclusive coletado parecer da Advocacia-Geral da União (AGU) sobre o assunto.[6] Em outros países, houve muita discussão em torno de aplicativos de rastreamento de contatos (*contact-tracing*). A falta de mobilização política a nível federal, entretanto, desacelerou, senão esvaziou, maiores esforços nesse sentido no Brasil.[7] Neste contexto, vale notar de pronto que nenhuma das medidas a serem analisadas se referiam diretamente a uma medida de *controle e combate* à doença tão direta como é o caso das ações de agentes de saúde no ingresso em domicílios. A do caso IBGE é apenas incidental ao contexto da pandemia; a do SIMI, apesar de inserida em uma estratégia de vigilância, não foi ambiciosa em termos de combate e controle – como veremos.

Isto posto, essa seção recuperará os aspectos principais das controvérsias judiciais que se desdobraram por conta dessas medidas. Como pretendo delinear, a discussão sobre o acesso de dados pelo IBGE obrigou o Supremo Tribunal Federal (STF) a discutir e assentar diversos princípios tradicionais que norteiam o direito da proteção de dados pessoais. Já a discussão sobre o SIMI, do Governo do Estado de São Paulo, consistiu, notadamente, na pergunta: o Estado ou as operadoras de telefonia estão violando o direito à privacidade dos portadores de celulares? Os casos ajudam a ilustrar as diferentes vocações dos direitos à privacidade e à proteção de dados pessoais.

a. STF, IBGE e o direito à proteção de dados pessoais

A MP 954 dispôs que "as empresas de telecomunicação prestadoras do STFC [Serviço Telefônico Fixo Comutado] e do SMP [Serviço Móvel Pessoal] deverão disponibilizar à Fundação IBGE, em meio eletrônico, a relação dos nomes, dos números de telefone e dos endereços de seus consumidores, pessoas físicas ou jurídicas" (art. 2º). Com respeito à finalidade do compartilhamento, previu que "os dados de que trata o caput serão utilizados direta e exclusivamente pela Fundação IBGE para a produção estatística oficial, com o objetivo de realizar entrevistas em caráter não presencial no âmbito de pesquisas domiciliares" (art. 2º, §Iº). Nesse sentido, assentou que essa finalidade seria exclusiva (art. 3º, II) e que não poderia haver sub-compartilhamentos com outros órgãos, entidades e empresas (art. 3º, §Iº), vedando-se ainda a utilização para fins de prova em qualquer tipo de processo (art. 3º, III). No mais, estabeleceu que a medida se aplicaria durante a pandemia (art. Iº, parágrafo único), que o IBGE informaria as hipóteses de uso e divulgaria relatório de impacto em proteção de dados (art. 3º, § 2º) e que os referidos dados deveriam ser excluídos assim que superada a situação de emergência (art. 4º).

A MP foi objeto de cinco ações diretas de inconstitucionalidade no STF (ADI 6387, 6388, 6389, 6390 e 6393), propostas pelo Conselho Federal da OAB, pelo PSDB, pelo PSB, pelo PSOL e pelo PCB. Tais ações mereceriam estudo próprio sobre suas nuances, manifestações de diferentes autoridades e intervenções de amigos da corte. Entretanto, aqui serão apresentadas de forma objetiva apenas para atender aos fins desse artigo.

Em síntese, sustentaram que a MP instituiria uma "estrutura contemporânea de vigilância da população", e que a concentração de dados facilitaria abusos e vazamentos e outras "ilegítimas interferências" sobre as pessoas. Implicaria desrespeito a princípios elementares do direito à proteção de dados pessoais, que poderiam ser extraídos das proteções constitucionais da intimidade e do sigilo de dados e do remédio do habeas data. A Advocacia-Geral da União, o Ministério Público Federal e o IBGE, por sua vez, defenderam que não se poderiam pressupor que haveria uso abusivo, que a MP envolveria apenas dados cadastrais e que não seria hipótese de quebra de sigilo, mas sim de "transferência de sigilo" (de empresas para o IBGE).

Para os propósitos desse texto, convém destacar o posicionamento bastante contundente do STF sobre o assunto. O voto da relatora Min. Rosa Weber manejou, de forma sofisticada, diversos aspectos de proteção de dados, desde a suspensão liminar – referendada pelo Plenário[8]. Acolhendo diversos pontos da tese trazida pelo PCB em sua inicial, assentou que também os dados que foram objeto do pedido são protegidos constitucionalmente e que a medida, com escopo ambíguo e alcance excessivo, não poderia ser admitida. A finalidade declarada – "produção de estatística oficial" – seria inespecífica, o que comprometeria também a avaliação sobre o atendimento do princípio da necessidade. Ademais, não teria sido elencada qualquer indicação da necessidade de uma coleta massiva de todos os dados, principalmente para pesquisas que, segundo o próprio IBGE declarou, seriam feitas por amostragem. Nesse aspecto, sinalizou que as principais pesquisas já estavam sendo realizadas remotamente, por dados já existentes. Por fim, também observou que não foram previstas medidas de segurança. Todos esses problemas seriam potencializados pela ausência de uma autoridade de controle e supervisão – visto que a Autoridade Nacional de Proteção de Dados prevista na Lei nº 13.709/18 ainda não foi criada – e pelo adiamento da entrada em vigor da Lei Geral de Proteção de Dados.

A relatora foi seguida pela maioria. De forma complementar e contextual às observações da relatora, vale destacar a manifestação do Min. Edson Fachin acerca da dimensão procedimental de direitos. No caso concreto, nem a excepcionalidade da crise vivida em razão da pandemia nem a necessidade de produção estatística justificaria a violação de direitos na forma pretendida. Seria sim, em tese, possível, mas apenas a partir de um reforço das garantias de natureza procedimental – conjunto de filtros e salvaguardas. Já o voto do Min. Gilmar Mendes fez questão de pontuar que as preocupações lançadas com a MP estão imbricadas com o reconhecimento de um direito fundamental à proteção de dados pessoais – restrições a esse direito estão submetidas à observância de princípios e parâmetros concretos, sob pena de serem inaceitáveis. Apenas o Min. Marco Aurélio discordou: entendeu haver "razão suficiente" para o compartilhamento de dados entre teles e IBGE e que ele não seria submetido a prazo indeterminado.[9]

b. Sistema de Monitoramento Inteligente em São Paulo

Outra discussão sobre acesso e uso de dados que ganhou repercussão durante a pandemia decorreu do "Sistema de Monitoramento Inteligente" (SIMI), do Governo do Estado de São Paulo – plataforma de acompanhamento de índices de adesão ao isolamento social a partir de informações de deslocamento de telefones celulares produzidas por empresas de telecomunicações. O índice seria medido pelo contraste entre a localização de celulares – medida com base na Estação Rádio Base (torre) com que estão conectados – em período noturno (22h às 02h) e a localização ao longo do dia: caso houvesse alteração, considerar-se-ia que não foi observado isolamento social (Glasmeyer, 2020; Zanatta, Bioni, Keller, & Favaro, 2020). Apenas o resultado da avaliação agregada seria compartilhado com o Governo.

O anúncio do sistema se deu em 9 de abril de 2020 em coletiva de imprensa[10], relatando que "a parceria com as operadoras de telefonia Vivo, Claro, Oi e TIM usa dados digitais para medir a adesão à quarentena em todo o Estado e também envia mensagens de alerta para regiões com maior incidência da COVID-19." Também se acrescentou que "não há ameaça à privacidade dos usuários, uma vez que não são analisadas as trajetórias individualmente e todos os dados são anonimizados e apresentados de forma agregada". Mais tarde, no mesmo dia, Doria afirmou em entrevista a programa de televisão que não descartariam medidas mais rigorosas, como pena de prisão, caso o índice de isolamento apontado pelo sistema não alcançasse a 60% e as pessoas não observassem a recomendação de isolamento social, reportaram diversos canais de notícia[11].

O saldo das duas declarações no mesmo dia foi o de numerosas ações judiciais. Em dois dias, já existiam ao menos dois *habeas corpus* no Superior Tribunal de Justiça, um deles individual (HC 572959), outro também em favor de toda a população de São Paulo (HC 572996), baseados nos dois conjuntos de notícias (sistema de monitoramento e menção à prisão), para que o uso de dados dos impetrantes cessassem e sua liberdade de ir e vir fosse assegurada de ameaças.

No segundo deles, a Min. Laurita Vaz[12] logo indeferiu a inicial por (i) impugnar a mera possibilidade de um constrangimento, "sem que haja elementos categóricos de que maneira a suposta ameaça ao direito ambulatorial materializar-se-ia", (iii) não tornar individualizáveis aqueles que se beneficiariam do HC coletivo; e (iii) questionar um ato em tese (medida governamental) – razões que tornariam o habeas corpus sequer passível de ser conhecido. Ainda assim,

sobre o mérito, registrou que: "Ainda que sejam relevantes as questões relativas ao direito de privacidade que podem ser levantadas em razão do compartilhamento de informações obtidas pelas empresas a partir da localização de aparelhos de telefonia celular, (...), o que há de concreto é que tanto o Governo estadual, como as operadoras de telefonia celular, esclarecem que no sistema implementado os usuários não são especificadamente individualizados." No primeiro habeas corpus, o Min. Napoleão Nunes Maia Filho chegaria à mesma conclusão.[13]

Foi também impetrado mandado de segurança[14] no Tribunal de Justiça de São Paulo (Processo nº 2073904-24.2020.8.26.0000, notadamente), também contra o Governador, sustentando violação à privacidade e à liberdade de ir vir – outra vez fundada nos pronunciamentos que viraram notícias – e portanto a necessidade de suspensão do SIMI e declaração de que a conduta configurou crime de responsabilidade. Em 17 de junho, o Órgão Especial denegou a ordem.

A partir de informações trazidas pela Procuradoria Geral do Estado (PGE) acerca dos termos do acordo de cooperação, assentou que "são repassadas ao Governo do Estado de São Paulo informações agregadas e anônimas, não sendo possível identificar quem são os usuários da operado [sic] de telefonia que estão conectados." Como se trata de "dados anônimos", não se verificaria ofensa aos "princípios da inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à intimidade". Não haveria "quebra de sigilo de dados telefônicos, tampouco no que diz respeito às conversações telefônicas". Impossível seria a possibilidade de efetuar prisão de pessoas assim. Tais dados "já são compartilhados" entre as empresas para 'viabilizar estudos para a melhoria da infraestrutura dessas empresas". Citou ainda o art. 72 da Lei nº 9.472/97 (Lei Geral de Telecomunicações) pela qual "a prestadora poderá divulgar a terceiros informações agregadas sobre o uso de seus serviços, desde que elas não permitam a identificação, direta ou indireta, do usuário, ou a violação de sua intimidade" e, também, parecer da AGU[15] em consulta do Ministério da Saúde sobre o tema, além da decisão da Min. Laurita Vaz. O sigilo dos dados então ficaria preservado pelo "anonimato e agregação das informações". Tendo assim concluído, ainda avançou dizendo que se entendesse que isso representasse uma ofensa à intimidade, a preservação do direito à saúde e da própria vida também levaria à denegação da ordem.

Analisando o tema sob outra perspectiva –– no âmbito de ações populares, são relevantes algumas decisões liminares de juízos de Varas da Fazenda Pública, inclusive antes de as impugnações serem concentradas por conexão processual. Em uma delas (Processo nº 1019257-34.2020.8.26.0053), sustentou-se violação aos princípios da publicidade e da transparência, já que o acordo que deu origem ao SIMI não foi publicado em diário oficial – não havendo clareza sobre seu escopo e as condições – que dados fazem parte do sistema, como ocorre o acesso, se há anuência dos titulares, se há garantia de que não serão usados para outras finalidades. Daí também decorreriam violações à legalidade e à moralidade administrativa; já a violação à privacidade decorreria do acesso a dados de celulares sem autorização ou ordem judicial. A 1ª Vara da Fazenda Pública acolheu parcialmente o pedido[16], determinando que os termos da parceria fossem trazidos aos autos – postergando a análise da existência de violação concreta à privacidade. A Procuradoria-Geral do Estado então juntou aos autos os termos do acordo e nota técnica do Instituto de Pesquisas Tecnológicas (IPT). A seguir, os autos foram remetidos à 4ª Vara da Fazenda Pública, para onde foi originalmente distribuído processo sobre o tema. O juiz entendeu que a parte que diferenciava essa ação das demais já havia sido atendido e a extinguiu, sem resolução de mérito no quanto excedente.[17]

Em 5 de maio de 2020, o SIMI foi instituído oficialmente pelo Decreto nº 64.963/2020 que previu que "destina-se a apoiar a formulação e avaliação das ações do Estado de São Paulo para enfrentamento da pandemia da COVID-19" e que "não conterá dados pessoais, assim considerados aqueles relacionados a pessoa natural, identificada ou identificável, limitando-se a dados anonimizados."

4. Novo cenário e complexidades conceituais

O direito à proteção de dados pessoais encontrou seu campo de aplicação ideal na pandemia do COVID-19. No cenário de alta inovação tecnológica em que já estávamos, não parecia razoável que precisássemos de uma pandemia para tanto, mas o fato é que a racionalidade procedimental desse ramo do direito manifestou-se com força (Zanfir-Fortuna, 2020), em toda sua complexidade e nas suas aproximações e diferenças em relação ao direito à privacidade.

Como visto de início, o direito à privacidade, inclusive na forma concretizada e específica do direito à inviolabilidade do domicílio, diz respeito à proteção de certos domínios privados do indivíduo. Não impõe uma divisão insuperável, mas confere a prerrogativa substantiva aos indivíduos para que decidam quem vai ingressar ou ter acesso a determinada esfera íntima, da sua vida privada (Ferraz Junior, 1993; Gellert & Gutwirth, 2013). Em meio a graves epidemias, a compreensão que prevaleceu é de que esse direito oponível ao Estado não é violado pelo ingresso motivado por razões de saúde pública, sobretudo quando regulado em lei de forma que não comprometa de forma excessiva o valor a que serve esse direito; mas pelo contrário, que o prestigie e tente acomodá-lo contra precipitações e abusos que possam decorrer dessa autorização.

Por sua vez, o direito à proteção de dados pessoais se refere ao próprio endereçamento de um conjunto de preocupações com riscos decorrentes da automação que se traduziu ao longo do tempo em princípios e salvaguardas que devem ser observadas para que o processamento ocorra de forma legítima e válida (Doneda 2006; Ruaru, Rodriguez e Finger, 2011; Gellert e Gutwirth, 2013; Mendes, 2014). Associa-se a noções de transparência, de vinculação à finalidade, de limitação do uso à adequação e necessidade, de observância de mecanismos de segurança, de responsabilização e de justificação em uma base legal, por exemplo. Refere-se a noções básicas de justiça no uso de dados. É um ramo do direito que constitui em si uma proteção regulatória que é exigida pelas situações de vulnerabilidade em que o titular de dados é posto em sua autodeterminação ao ser submetido a essa relação informacional de poder com o Estado – ainda que a operação de tratamento em si não viole direito individual.

Em outras palavras, as crises epidemiológicas mostram como existe uma dimensão substantiva de direitos que convive com as respectivas proteções regulatórias contras riscos e possíveis abusos. Enquanto o direito à privacidade tem a sua dimensão substantiva já consagrada, o direito à proteção de dados pessoais é mais notável pela dimensão procedimental que o acompanha. Nos dois casos, entretanto, verificam-se as duas dimensões: o direito à privacidade do lar convive com procedimentos que prestigiam o valor subjacente contra abusos em nome de epidemia; o direito da proteção de dados pessoais está comprometido com uma concepção de autodeterminação que barra oportunismo e irresponsabilidade do Estado no tratamento de dados pessoais, também mesmo em meio a crise de saúde pública. Feita essa observação, é também certo como operam com escopo e ênfase distintas: um protege aspectos da vida

privada contra acessos de terceiros; outro, a justiça de relações informacionais.

Com frequência, a confusão entre os dois direitos esfumaça a própria natureza de controvérsias. Como se viu nos dois casos analisados no tópico anterior, uma pergunta fundamental era se havia violação à *privacidade e à intimidade*, nas concepções tradicionais desses termos, gestadas sob a lógica da separação entre domínio público e domínio privado. Veja-se o primeiro caso: compartilhar com terceiros dados de nome, endereço e número de telefone fere a privacidade das pessoas – essas são informações que revelam algo íntimo? Mesmo se ocorrer "transferência de sigilo" – o novo recebedor se compromete a guardar sigilo? Era, em certo sentido, inevitável que a demanda recorresse à linguagem e aos fundamentos do direito à privacidade de forma reflexiva e com ela consistente. Afinal, o que seus autores pretendiam era o reconhecimento de um direito não-explícito na Constituição Federal de 1988 (a *proteção de dados pessoais*), de modo que era necessário construí-lo a partir de bases já conhecidas (como a de *privacidade*).

No entanto, as perguntas que indiquei, mobilizadas inclusive na argumentação do MPF e da AGU sob a lógica da privacidade, são enganosas e insuficientes ao caso: ainda que seja respondido que não há violação a um domínio privado/íntimo, diversas outras questões decorrentes do uso de dados pessoais permanecem. Por exemplo: qual a finalidade do compartilhamento? Como vai ser operacionalizado o compartilhamento e o uso? É mesmo necessária essa escala massiva, abrangendo todos os clientes? Que medidas de segurança foram adotadas? É justamente a ausência de resposta suficiente e adequada a essas últimas perguntas que configuram a ilicitude da medida no caso do compartilhamento com o IBGE.

Essa dinâmica entre privacidade e proteção de dados talvez fique ainda mais clara no segundo caso. Desde o início, a controvérsia foi alimentada por uma profunda falta de clareza sobre o funcionamento do SIMI. A questão de mérito em jogo nas diversas demandas era se o sistema violava a privacidade – um domínio privado dos indivíduos, que têm o direito de deixar fora do conhecimento de terceiros (incluindo o Estado) pelo monitoramento da localização. A partir de informações mais robustas e demonstração documental dos termos do acordo de cooperação técnica e da funcionalidade do sistema, a existência de uma violação à privacidade foi descartada: não passavam de dados anonimizados e agregados, não oferecem um retrato individualizado sobre mobilidade de indivíduos. Superada essa pergunta sobre privacidade, sob a lógica da proteção de dados pessoais, permanece a pergunta: mas haveria algum princípio ou salvaguarda de proteção de dados a ser observada?

Como chegou a explorar a PGE, a Lei Geral de Proteção de Dados ainda entraria em vigor – e, ainda que já estivesse, não seria aplicável por se tratarem de dados anonimizados. A observação é válida, mas não afasta outras avaliações: de pronto, em atenção ao princípio da transparência, os atores envolvidos deveriam ter dado publicidade ao modelo de uso de dados e a anonimização das informações, que afastaria a aplicação da LGPD. Deveria haver ampla publicidade sobre os termos da medida e demonstrações de que efetivamente foram tomadas medidas razoáveis que não sujeitariam os dados envolvidos a processos de reidentificação (Machado & Mendes, 2020), por exemplo.

Essas, aliás, foram as observações que fez o *European Data Protection Supervisor*, Wojciech Wiewiórowski à Comissão Europeia no contexto de iniciativas para uso de dados de geolocalização para monitoramento de isolamento social, "para que se evitem mal-entendidos" (Wiewiórowski, 2020). Esse próprio exemplo mostra como a existência de *encarregados de proteção de dados* e de *autoridades competentes* na matéria servem para gerar confiança sobre

a integridade de certas aplicações que envolvem uso de dados pessoais. Se algo semelhante já existisse no Brasil, é pouco provável que a controvérsia tivesse tomado a proporção que tomou. Sem essa sofisticação, tornou-se alvo fácil de disputa mais politicamente carregada do que técnica juridicamente (Langenegger & Bottino, 2020).

5. Lições da pandemia

Como se viu, proteção de dados é um ramo do direito notadamente responsável por canalizar procedimentos que envolvem uso de dados pessoais, minimizando riscos e abusos pela imposição da observância de regras e princípios e pela estruturação de mecanismos de supervisão e controle.

Ilustrado o seu caráter em contraste com a privacidade, esta seção faz observações específicas sobre a interação desse direito com políticas públicas de proteção da saúde pública – que se mostram relevantes para o enfrentamento dessas discussões jurídicas sobre acesso a dados na pandemia, mas que são relevantes também para todo o debate sobre garantias constitucionais daqui adiante. Ao menos três lições podem ser tiradas.

a. Encontro entre precauções

A primeira lição é que a pandemia da COVID-19 ilustrou um encontro entre duas aplicações do "princípio da precaução": de um lado, o que motiva a vigilância em saúde; do outro, o que permeia a proteção de dados pessoais.

O princípio da precaução se refere a um tipo de abordagem regulatória que teve origem principalmente na área de direito ambiental para lidar com situações de risco e ameaças em um cenário de incerteza científica (Costa, 2012, p. 15-6; Bioni & Luciano, 2019, p. 209-14). Nasce de uma postura de prudência com relação ao desenvolvimento científico e tecnológico – e que deve nortear tanto a tomada de decisões quanto o acompanhamento das consequências dela (Aith & Dallari, 2009, p. 102; Narayanan, Huey e Felten, 2016, p. 371).

No campo de saúde é compreendido como fator motivador da criação de estruturas de vigilância em saúde para proteção e prevenção de possibilidades de danos à saúde de pessoas – "trata-se de vigilância calcada na precaução sobre riscos incertos e desconhecidos que podem aparecer em decorrência das características que cercam a vida do ser humano no globo terrestre (um novo vírus, um terremoto, uma enchente)" (Aith & Dallari, 2009, p. 105). Na Constituição Federal brasileira, está presente notadamente no art. 200, que atribui competências ao Sistema Único de Saúde, entre elas a de "executar ações de vigilância sanitária e epidemiológica".

Já na área de proteção de dados pessoais, o princípio tem sido cada vez mais utilizado para se referir e explicar uma nova "moldura teórica" (Zanatta, 2018) desse ramo do direito, que vê nele o propósito de mitigar riscos decorrentes do uso de informações pessoais (Costa, 2012; Gellert & Gutwirth, 2013; Gellert, 2015). Parte de uma compreensão da área menos presa à lógica individualista de um "direito à autodeterminação informacional", e mais focada nos aspectos coletivos da proteção e prevenção de riscos que pretendem ser alcançados por leis gerais que condicionam e balizam operações de tratamento de dados, e instituem mecanismos como *privacy by design* e relatórios de impacto.

Nesse contexto, há incidência de dois direitos de índole *social* – saúde e proteção de dados –, que exigem do Estado ações concretas de promoção e defesa ativa. Enquanto o direito social à saúde já é paradigmaticamente reconhecido nesse sentido, o direito à proteção de

dados pessoais vem passando por esse processo de afirmação. Os casos estudados acima apontam para esse sentido: ações estatais, mesmo em contexto de crise epidemiológica, devem ser capazes de conviver com e respeitar parâmetros de proteção de dados pessoais. É necessário um esforço de acomodação mútua: da proteção de dados para os interesses de saúde pública, e da saúde pública para as preocupações com proteção de dados. Nesse sentido, é de se esperar, na linha do que fez o STF quando interesses de proteção à saúde pública e ao meio ambiente precisaram ser conciliados[18], que medidas empregadas para vigilância e controle sanitário que envolvam dados pessoais devam necessitar no futuro de aprovação não apenas de autoridades sanitárias, mas também da autoridade nacional de proteção de dados para que possam ser implementadas.

b. Legalidade

A segunda lição é sobre a relevância do princípio da legalidade para estabelecer limites ao poder do Estado sobre o uso de dados pessoais mesmo em contexto de crise epidemiológica.

Caro ao direito administrativo, impõe à Administração Pública o dever de atuar segundo os ditames e previsões em Lei, não sendo possível criar obrigações, conceder direitos ou impor vedações de qualquer espécie sem autorização legal. Nesse sentido, também constrange o poder de polícia *sanitário* – "a faculdade que tem a administração pública para, por meio de suas autoridades sanitárias, limitar ou disciplinar direito, interesse ou liberdade, regulando a prática ou abstenção de ato, em razão de interesse público concernente à detecção, prevenção e controle de riscos de doenças e de agravos à saúde" (Aith & Dallari, 2009, p. 115).

O princípio é também de suma importância na proteção de dados. O modelo europeu, no qual o brasileiro se inspirou, exige que cada operação de "tratamento de dados"[19] seja justificada por uma "*base legal*" – uma hipótese autorizadora. Para a Administração Pública, de forma específica, existe a base legal da necessidade à "execução de políticas públicas previstas em leis ou regulamentos" (Lei nº 13.709/2020, arts. 7º, III; II, II, b) [20]. Supõe-se ainda a possibilidade de uso de dados para "executar as competências legais ou cumprir as atribuições legais do serviço público" (art. 23) (Wimmer, 2021a). A operação de tratamento deve estar, portanto, vinculada a política pública ou a competência ou atribuição prevista em lei. "Regulamentos" do Executivo são também em princípio admitidos – mas estes também só são válidos se tiverem base em autorização legal.

Há ainda previsão de justificativa com base na "tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou *autoridade sanitária*" (arts. 7, VIII e II, II, f), que a princípio não faz referência à necessidade de que a medida de tutela da saúde tenha previsão legal. De forma consistente com o direito administrativo, a utilização dessa base legal, no que se refere à atuação de autoridade sanitária, só pode ser interpretada de modo a supor a existência de competência legal da autoridade sanitária para a atividade de tutela da saúde em questão – principalmente em situações de emergência concreta e imediata à saúde de alguém, na linha do que inclui profissionais e serviços de saúde. No final das contas, trata-se, nesse aspecto, de uma base legal específica, mas que é contemplada pelas anteriores sob a compreensão de que a atuação da autoridade sanitária se circunscreve a competências e atribuições legais de uma política pública em saúde em que suas atividades estão inseridas.

Nesse contexto, medidas de vigilância e controle epidemiológico que envolvem restrições a direitos devem ter previsão legal (Aith & Dallari, 2009, p. 121; Teixeira; Costa, Viana e Paim, 2009, p. 133-4). Essa consideração já estava presente nos debates sobre o ingresso

forçado em domicílios e que resultou na aprovação da lei federal com delimitação específica das hipóteses em que essa possibilidade seria legítima (Azevedo, 2002, p. 122). É uma medida necessárias para que não haja onerosidade excessiva ao titular na situação de vulnerabilidade em que é/será posto; para contenção de possíveis abusos.

No contexto do uso de dados pessoais para combate à pandemia, voltou à tona a discussão sobre quão precisa e específica essa previsão deve ser: muito embora a legalidade estrita em si não estivesse imediatamente em questão por envolver uma medida proposta por medida provisória, foram explícitas as mensagens do STF quanto à imprecisão da MP do IBGE quanto à finalidade a ser dada, que comprometia a própria validade da medida (em especial sobre sua necessidade). A previsão legal não atendeu aos parâmetros mínimos necessários para autorizar medida dessa natureza.

Digno de nota é também a articulação de argumentos que questionaram o SIMI por falta de previsão legal – questionando que algo desse tipo pudesse ser inserido em uma prerrogativa geral da administração de poder de polícia para segurança em saúde. Com efeito, nessas circunstâncias utilizam-se um conjunto de dados gerados por conta e em razão da provisão de serviço de telefonia em finalidades diferentes segundo solicitação do Poder Público. Por, no final das contas, estar fundado em uma ação voluntária de empresas e não envolver dados pessoais, o ponto correu por fora da discussão, mas ainda assim foi articulado e suscita questão importante.

Nesse contexto, está clara uma agenda de pesquisa sobre o princípio da legalidade e as bases legais que recorrem ao *interesse público* para tratamento de dados pessoais na execução de políticas públicas e competências e atribuições legais: quão específicas devem ser dispositivos legais que autorizem uso de dados? No caso da restrição à privacidade no ingresso forçado a domicílio, a restrição a direito era mais evidente e houve anos de discussão até a aprovação de lei federal específica. Quão específica deve ser a previsão quando envolver uso de dados pessoais? E quanto admite especificação infralegal, por regulamento? A lógica de precaução por princípios e salvaguardas da proteção de dados deve balizar a discricionariedade administrativa nesse contexto.

Cabe aqui uma observação sobre um parâmetro básico: não se pode supor que dados não relacionados à saúde possam ser objeto de acesso generalizado para fins de vigilância sanitária nem que medidas não diretamente relacionadas ao combate sejam admissíveis a partir de normas genéricas. A fundamentação para o exercício do poder de polícia sanitário deve ser tanto mais forte e exigente quanto a medida se distancia dos paradigmas de vigilância sanitária – passe a envolver mais coleta e uso de dados pessoais, cooperação com agentes privados que não sejam do setor de saúde, e aplicações tecnológicas experimentais sem comprovação de eficácia direta no combate à doença. De início, portanto, medidas dessa natureza devem envolver norma específica.

O ponto é importante porque serve para delimitar o escopo de um dos dispositivos da Lei nº 13.979/2020 – que dispõe sobre medidas de enfrentamento da pandemia. Na referida lei foi incluído um dispositivo que obriga compartilhamento de informações de identificação de pessoas infectadas e casos suspeitos entre órgãos e entidades da administração pública. Dispõe o art. 6º que "*É obrigatório o compartilhamento entre órgãos e entidades da administração pública federal, estadual, distrital e municipal de dados essenciais à identificação de pessoas infectadas ou com suspeita de infecção pelo coronavírus, com a finalidade exclusiva de evitar a sua propagação*". O § 1º prevê que "*A obrigação a que se refere o caput deste artigo estende-se às pessoas jurídicas de direito privado quando os dados forem solicitados por autoridade sanitária*". *Já o § 2º, que "O Ministério da Saúde manterá dados*

públicos e atualizados sobre os casos confirmados, suspeitos e em investigação, relativos à situação de emergência pública sanitária, resguardando o direito ao sigilo das informações pessoais."

Sob a perspectiva do direito administrativo e da proteção de dados pessoais, esse dispositivo serve bem para justificar o compartilhamento de informações sobre pacientes que alimentam as estatísticas sobre o COVID-19 no Brasil e o monitoramento do avanço da doença. As estatísticas são divulgadas de forma que não se identifica ninguém, mas para que elas possam ser geradas de forma organizada e até estudadas por centros de pesquisa, é necessário que haja coleta (independente de consentimento do paciente) em nível integrado entre unidades de saúde, laboratórios, públicas e privadas, e secretarias de saúde, a nível municipal, estadual e federal.

Desse dispositivo não se poderia extrair, entretanto, que solicitações de acesso a dados que nada tem a ver com o sistema de saúde, inclusive detidos por agentes privados – como as de telefonia e geolocalização obtidos e custodiados por empresas para outras finalidades – atenderiam à exigência de previsão legal específica. Com efeito, a área de vigilância epidemiológica é voltada preponderantemente para a coleta e análise de informações de saúde *em primeiro grau*, por assim dizer, sobre a ocorrência de doenças transmissíveis e agravos à saúde em si. Tanto que uma das fontes principais do monitoramento é a notificação compulsória – prevista no art. 7º da Lei nº 6.259/75.[21] Na versão atual, há dever de notificar[22] doenças, agravos e eventos de saúde listados na Portaria de Consolidação nº 4, de 28 de setembro de 2017, do Ministério da Saúde, que inclusive já continha obrigações de monitoramento de síndrome respiratória aguda grave associadas a coronavírus. Essas informações são também usadas para medidas concretas de controle – como para que o paciente observe quarentena. Esse paradigma deve, portanto, seguir a interpretação de normas gerais. Nesse sentido, o acesso a dados estranhos a finalidades de saúde, coletados sob outros contextos e regramentos, nunca se poderia supor possível automaticamente sem previsão legal específica.

O mesmo vale para a leitura do art. 45, §2º do Decreto nº 10.212/2020, que internalizou o Regulamento Sanitário Internacional de 2005. Tal dispositivo previu que "Estados Partes poderão revelar e processar dados pessoais quando isso for essencial para os fins de avaliação e manejo de um risco para a saúde pública", na mesma linha, me parece que o dispositivo de que tratei acima sobre tutela da saúde por autoridades sanitárias. De forma específica, dispõe ainda que "no entanto os Estados Partes, em conformidade com a legislação nacional, e a OMS devem garantir que os dados pessoais sejam: (a) processados de modo justo e legal, e sem outros processamentos desnecessários e incompatíveis com tal propósito; (b) adequados, relevantes e não excessivos em relação a esse propósito; (c) acurados e, quando necessário, mantidos atualizados; todas as medidas razoáveis deverão ser tomadas a fim de garantir que dados imprecisos ou incompletos sejam apagados ou retificados; e (d) conservados apenas pelo tempo necessário". Como se vê, o dispositivo nunca poderia ser entendido como uma prerrogativa genérica para uso de dados, mas apenas balizadora de como o uso deve ser feito.

c. Divisão informacional de poderes e integridade nos fluxos de dados

A terceira lição, relacionada, é sobre divisão informacional dos poderes. Esse é um dos princípios que servem para sustentar uma sociedade baseada na coleta e uso de dados de forma democrática: o que cada entidade pode fazer com

dados se circunscreve à finalidade da coleta e à sua competência.[23] Isso vale dentro do governo, mas também quando estamos falando de fluxo de dados entre entes públicos e privados sob a perspectiva da integridade contextual[24]. Aparece muito forte com a LGPD e o princípio da finalidade (art. 6º, I). O fato de que não existe um livre fluxo de dados, e que bases de dados não podem ser facilmente usurpadas de um agente pelo e para o outro, é uma garantia democrática; é um mecanismo de contenção de poder. Serve para que avancemos com a tecnologia e serviços baseados em dados, com relativa segurança de que não estamos avançando para nos tornar um Estado de vigilância em massa.

Então, não é porque um banco de dados existe dentro de uma estrutura de governo ou porque uma empresa tem certa estrutura, que automaticamente podem ser apropriados – nem mesmo a pandemia autorizou esse tipo de desvirtuação no Brasil e ao redor do mundo.[25] Possibilidades de compartilhamento devem estar sujeitas a situações compatíveis, dentro das expectativas de titulares de dados e dentro de hipóteses legais específicas (Wimmer, 2021b).

E, na medida em que possíveis, é muito importante que, como qualquer outra medida de saúde pública, seja (i) transparente, formulada com amplo diálogo com e participação da comunidade; (ii) baseada em evidências de eficácia para a contenção da doença – como é o caso do controle vetorial feito com relação à dengue e que justifica a restrição pontual e excepcional a direito; (iii) paralela à existência de capacidade de análise e resposta dos sistemas de saúde às informações levantadas[26]; e, sem a pretensão de esgotar[27], (iv) temporária – aplicável só para a emergência de saúde.

6. Conclusão

Como se viu, a pandemia do COVID-19 trouxe reflexões sobre os limites da atuação estatal com respeito ao uso de dados pessoais, assim como fez a epidemia de dengue/zika com respeito à privacidade do domicílio. A aproximação entre esses dois momentos permite enxergar tanto os pontos de aproximação como as diferenças no funcionamento e nas racionalidades do direito à privacidade em comparação ao direito da proteção de dados pessoais: aquele voltado à proteção da intimidade, este à observância de noções básicas de justiça no tratamento de dados pessoais.

Enquanto o direito à privacidade é mais conhecido por sua dimensão substantiva, mas não deixa de ser apoiado por proteções regulatórias também baseadas em procedimentos diante de medidas estatais que possam ameaça-lo, o direito à proteção de dados pessoais se confunde com sua própria dimensão procedimental – traduz-se e ganha reconhecimento como aparato regulatório para conter riscos de diversas espécies que podem decorrer do tratamento de dados pessoais.

A experiência do Brasil com relação a uso de dados na pandemia – embora não tenha sido inovadora nem agressiva – tanto permite ilustrar essa dimensão procedimental quanto lança luz sobre debates que precisam ser avançados no tratamento de dados pelo poder público de forma geral e no contexto de políticas de saúde pública em particular, e, portanto, sobre importantes agendas de pesquisa. Há muito trabalho pela frente, mas noções importantes vieram para ficar.

Referências

Aith, F. & Dallari, S. G.. Vigilância em Saúde no Brasil: Os Desafios dos Riscos Sanitários do Século XXI e a Necessidade de Criação de um Sistema Nacional de Vigilância em Saúde. Revista de Direito Sanitário, v. 10, n. 2, p. 94-125, Jul./Out. 2009.

Azevedo, P. F. Do combate ao Aedes Aegypti e a Liberdade do Proprietário ao Direito à Saúde. Revista de Direito Sanitário, vol. 3, n.2, pp. 107-23, Julho de 2002.

Bioni, B. & Luciano, M. O princípio da precaução na regulação da inteligência artificial: seriam as leis de proteção de dados o seu portal de entrada? In: Frazão, A. & Mulholland, C.. (Org.). Inteligência Artificial e Direito - Ética, Regulação e Responsabilidade. 1ed. São Paulo: Thomson Reuters, p. 207-231, 2019, p. 209-14.

Bioni, B., Zanatta, R., Monteiro, R. L. & Rielli, M. Privacidade e Pandemia: Recomendações para uso legítimo de dados no combate à Covid-19. São Paulo: Data Privacy Brasil, 2020.

Costa, L. Privacy and the precautionary principle. Computer Law & Security Review, vol. 28, pp. 14-24, 2012.

Doneda, D. Da Privacidade à Proteção de Dados Pessoais. Rio de Janeiro: Renovar, 2006.

Ferraz Junior, T. S.. "Sigilo de Dados: o direito à privacidade e os limites da função fiscalizadora do Estado". Revista da Faculdade de Direito da Universidade de São Paulo, vol. 88, 439–59, 1993.

Figueiredo, P., "Se não elevarmos isolamento para mais de 60%, tomaremos medidas mais rígidas', diz Doria; índice caiu para 49% em SP", G1, 9 de abril de 2020, disponível em: https://g1.globo.com/sp/sao-paulo/noticia/2020/04/09/se-nao-elevarmos-isolamento-para-mais-de-60percent-tomaremos-medidas-mais-rigidas-diz-doria-indice-caiu-para-49percent-em-sp.ghtml .

Fragoso, N., Roberto, E., Silveira, J.F. & Tavares, C. Privacy and Data Protection in the Pandemic: report on the Use of Apps and Alternative Measures in Brazil. São Paulo, InternetLab, 2021

Gellert, R. & Gutwirth, S.. The legal construction of privacy and data protection. Computer Law and Security Review, vol. 29, pp. 522-530, 2013.

Gellert, R. Data Protection: A Risk Regulation? Between the Risk Management of Everything and the Precautionary Alternative. International Data Privacy Law, vol. 5, nº 1 3–19, 2015.

Glasmeyer, R. A implementação do *Contact Tracing* e a montagem de vigilâncias na pandemia da Covid-19. Revista Internet & Sociedade, vol. 1, n. 1, pp. 200-220, 2020.

Greco, L. O inviolável e o intocável no direito processual penal: considerações introdutórias sobre o processo penal alemão (e suas relações com o direito constitucional, o direito de polícia e o direito dos serviços de inteligência). In: WOLTER, Jürgen. O inviolável e o intocável no direito processual penal: reflexões sobre dignidade humana, proibições de prova, proteção de dados (e separação informacional de poderes) diante da persecução penal. São Paulo: Marcial Pons, 2018, pp. 21-82.

Langenegger, N. & Bottino, C.. The Renewed Importance of Data – and Data Protection – in Times of COVID-19, Network of Centers, 22 de junho de 2020, disponível em: https://medium.com/the-network-of-centers-collection/the-renewed-importance-of-data-and-data-protection-in-times-of-covid-19-244ba8ed4831 .

Machado, D. C., & Mendes, L. S.. Tecnologias de perfilamento e dados agregados de geolocalização no combate à covid-19 no Brasil. Revista Brasileira De Direitos Fundamentais & Justiça, vol. 14, n. 1, 105-148, 2020.

Mendes, L. S.. Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014.

Mendes, L. S. & Keller, C. I.. A new milestone for data protection in Brazil. Internet Policy Review, 13 de maio de 2020, disponível em: https://policyreview.info/articles/news/new-milestone-data-protection-brazil/1471;

Narayanan, A.; Huey, J. & Felten, E. W. A Precautionary Approach to Big Data Privacy. In: Gutwirth, S.; Leenes, R.; De Hert, P.. Data Protection on the Move. New York: Springer,p. 357–385, 2016.

Nissenbaum, H. Privacy in Context: technology, policy, and the integrity of social life. Stanford: Stanford Univerity Press, 2010.

Pisaru, G., Zanatta, R. & Rielli, M. "Please do not share": Brazilian Federal Court Rules in Favor of Privacy, Access Now, 14 de maio de 2020, disponível em: <https://www.accessnow.org/brazilian-supreme-federal-court-rules-in-favor-of-privacy/>.

Ruaru, R., Rodriguez, D. F & Finger, B. O direito à proteção de dados e a privacidade. Revista da Faculdade de Direito – UFPR, n. 3, pp. 45-66, 2011.

Sarlet, I. W. & Weingartner Neto, J.. A inviolabilidade do domicílio e seus limites: o caso do flagrante delito. Revista de Direitos Fundamentais e Democracia, Curitiba, v. 14, n. 14, p. 544-562, julho/dezembro de 2013.

Sundfeld, C. A.. Vigilância epidemiológica e direitos constitucionais. Revista de Direito Sanitário, vol. 3, n. 2, pp. 90-106, Julho de 2002.

Teixeira, M. G., Costa, M. C. N., Viana, I. & Paim, J. Vigilância em Saúde: É necessária uma legislação de emergência? Revista de Direito Sanitário, v. 10, n. 2, p. 126-144, 2009, p. 130-1.

Trindade, R. App Coronavírus SUS agora vai avisar quando o usuário foi exposto; entenda, UOL, 31 de julho de 2020, disponível em: https://www.uol.com.br/tilt/noticias/redacao/2020/07/31/app-coronavirus---sus-adiciona-rastreamento-de-contatos-entenda.htm. A iniciativa permanece objeto de pouco encorajamento público de sua utilização.

Zanfir-Fortuna, G., "Why data protection law is uniquely equipped to let us fight a pandemic with personal data", pdpEcho, 6 de abril de 2020, disponível em https://pdpecho.com/2020/04/06/why-data-protection-law-is-uniquely-equipped-to-let-us-fight-a-pandemic-with-personal-data/ .

Zanatta, R. A. F. Proteção de dados pessoais como regulação do risco: uma nova moldura teórica? ***in***: I Encontro da Rede de Pesquisa em Governança da Internet. Rio de Janeiro: Rede de Pesquisa em Governança da Internet, 2018, pp. 175–193.

Zanatta, R., Bioni, B., Keller, C., & Favaro, I. Os Dados e o Vírus. Revista Brasileira De Direitos Fundamentais & Justiça, vol. 14, n. 1, 231-256, 2020.

Wiewiórowski, W. Carta do European Data Protection Supervisor a Roberto Viola, da Comissão Europeia, datada de 25 de março de 2020, disponível em: https://edps.europa.eu/sites/edp/files/publication/20-03-25_edps_comments_concerning_covid-19_monitoring_of_spread_en.pdf.

Wimmer, M.. O Regime Jurídico do Tratamento de Dados Pessoais pelo Poder Público. In: Doneda, D., Sarlet, I. W., Mendes, L. S. & Rodrigues Junior, O. L.. (Org.). Tratado da Proteção de Dados no Brasil, no Direito Estrangeiro e Internacional. 1 Ed. Rio de Janeiro: Forense, 2021a, pp. 271-288.

Wimmer, M. Limites e possibilidades para o uso secundário de dados pessoais no poder público: lições da pandemia. Revista Brasileira de Políticas Públicas, vol. 11, n. 1., pp. 122-142, 2021b.

Notas finais

1 A autora agradece a Caio Gentil Ribeiro, Maria Luciano e os pareceristas pelos comentários atentos, que contribuíram para o aperfeiçoamento do artigo.

2 Sobre a inviolabilidade do domicílio e suas exceções, ver Sarlet & Weingartner Neto, 2013.

3 Nos termos da Lei nº 8.080/90 (Lei Orgânica da Saúde), "Entende-se por vigilância epidemiológica um conjunto de ações que proporcionam o conhecimento, a detecção ou prevenção de qualquer mudança nos fatores determinantes e condicionantes de saúde individual ou coletiva, com a finalidade de recomendar e adotar as medidas de prevenção e controle das doenças ou agravos." (art. 6º, §2º).

4 Azevedo, 2002 (defendendo a necessidade de legislação específica sobre ingresso forçado); Sundfeld, 2002 (entendendo que a legislação existente que autoriza autoridades sanitárias a sujeitarem pessoas a medidas de controle já seria suficiente).

5 Refiro-me (i) à ADI 5592/DF, rel. Min. Cármen Lúcia, julgada em 04.04.2019, sobre a possibilidade de incorporação de mecanismos de controle vetorial por meio da dispersão por aeronaves (Art. 1º, §3º, IV), em que se deu interpretação conforme (por maioria); e (ii) à ADI 5581, rel. Min. Cármen Lúcia, sobre a concessão de benefícios previdenciários para vítimas de microcefalia, julgada prejudicada em 01.05.2020 por revogação do dispositivo.

6 BRASIL. Advocacia-Geral da União. Parecer nº 00281/2020/CONJUR-MCTIC/CGU/AGU, NUP 01250.015606/2020-12, de 02 de abril de 2020.

7 Ao tempo em que encerrava este artigo, foi anunciado que aplicativo do SUS passaria a utilizar tecnologia de *contact-tracing* (notificação de exposição de contatos). Cf. Trindade, 2020; Fragoso, Roberto, Silveira & Tavares, 2021. A iniciativa permanece objeto de pouco encorajamento público de sua utilização.

8 BRASIL. Supremo Tribunal Federal, Referendo da MC nas ADIs nº 6387, 6388, 6389, 6390 e 6393, j.. 7 de maio de 2020, DJe 12 nov. 2020. A sessão de julgamento pode ser visualizada em: <http://www.stf.jus.br/portal/cms/verNoticiaDetalhe.asp?idConteudo=442902#:~:text=O%20Plen%C3%A1rio%20do%20Supremo%20Tribunal,a%20pandemia%20do%20novo%20coronav%C3%ADrus.>. Para referência, ver também Mendes e Keller, 2020 e Pisaru, Zanatta e Rielli, 2020.

9 Os acórdãos com todos os votos e declarações de Ministros ainda não foram publicados, de modo que as observações feitas se referem aos comentários orais feitos durante a sessão.

10 A coletiva de imprensa de 9 de abril de 2020 com o Governador João Doria anunciando o programa pode ser visualizada em: https://www.youtube.com/watch?v=n9w_jdPPMRk . O anúncio também pode ser encontrado no site do Governo: "Governo de SP apresenta Sistema de Monitoramento Inteligência contra coronavírus", 9 de abril de 2020, disponível em: https://www.saopaulo.sp.gov.br/noticias-coronavirus/governo-de-sp-apresenta-sistema-de-monitoramento-inteligente-contra-coronavirus/.

11 "Se não houver neste final de semana consciência das pessoas, seja na capital de São Paulo ou em qualquer outra região neste fim de semana, nós estamos monitorando isso pelos celulares, a partir de segunda-feira o governo do estado de São Paulo tomará medidas mais rigorosas e mais duras, inclusive com a penalização de prisão para as pessoas que desobedecerem essa orientação; eu espero que não tenhamos que chegar a esse patamar", disse o Governador João Doria. Ver Figueiredo, 2020.

12 BRASIL. Superior Tribunal de Justiça, HC 572996, Min. rel. Laurita Vaz, decisão monocrática de 16 de abril de 2020.

13 BRASIL. Superior Tribunal de Justiça, HC 572959, Min. rel. Napoleão Nunes Maia Filho, decisão monocrática de 13 de maio de 2020.

14 BRASIL. Tribunal de Justiça de São Paulo, MS 2073904-24.2020.8.26.0000, rel. Alex Zilenovski. julgado em 17 de junho de 2020.

15 BRASIL. Advocacia-Geral da União. Parecer nº 00280/2020/CONJUR-MCTIC/CGU/AGU, NUP 01250.013581/2020-12, 01 de abril de 2020.

16 BRASIL. Juízo da 1ª Vara da Fazenda Pública da Comarca de São Paulo do TJSP, Ação popular nº 1019257-34.2020.8.26.0053, decisão de 15 de abril de 2020 (fls. 70-73).

17 BRASIL. Juízo da 4ª Vara da Fazenda Pública da Comarca de São Paulo do TJSP, Ação popular nº 1019257-34.2020.8.26.0053, decisão de 14 de maio de 2020 (fls. 360-1).

18 Refiro-me à ADI 5592/DF, rel. Min. Cármen Lúcia, julgada em 04.04.2019, sobre a possibilidade de incorporação de mecanismos de controle vetorial por meio da dispersão por aeronaves (Art. 1º, §3º, IV da Lei nº 13.301/16), em que o STF assentou por maioria a interpretação conforme no sentido de que "a aprovação de autoridades sanitárias e ambientais competentes e a comprovação científica da eficácia da medida são condições prévias e inafastáveis à incorporação de mecanismo de controle vetorial por meio de dispersão por aeronaves, em atendimento ao disposto nos arts. 6º, 196 e 225, § 1º, V e VII, da CF".

19 Lei nº 13.709/2020: "Art. 5º, X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

20 Lei nº 13.709/2020: "Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses: b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;".

21 Foi implantada à luz do Regulamento Sanitário Internacional de 1969 e instituída na ditadura militar em meio à epidemia de meningite meningocócita. Cf. Teixeira, Costa, Viana e Paim, 2009, p. 130-1. Como aponta Sundfeld, 2002, p. 95, a existência de mecanismos de notificação é bem antiga e remonta aos primeiros anos da República (como Decreto nº 68/1889).

22 O formulário a ser preenchido por médicos, profissionais de saúde e responsáveis por estabelecimentos de saúde envolve a coleta e transmissão de dados pessoais de pacientes, como nome, data de nascimento, sexo, estado gravídico, endereço, telefone e data de início dos sintomas.

23 "'Toda tentativa de enxergar a administração pública como uma unidade informacional é incompatível com uma proteção eficiente de dados'. Se saber é poder, o Estado não pode saber tudo, porque um Estado que tem conhecimentos ilimitados tem também um poder ilimitado. O direito de proteção de dados, que começa como direito subjetivo, mostra-se, ao menos em boa parte, como garantia institucional, relativa à própria estrutura da sociedade e do Estado. Nesse nível macro o direito se transforma em uma exigência de separação informacional dos poderes." Greco, 2018, p. 45.

24 Estou tomando o termo emprestado da teoria de Helen Nissenbaum, para me referir à preocupação de que fluxos de dados devem atender a noções do que é apropriado coletar e usar em certo contexto, quais os papeis dos atores envolvidos (de quem e para quem podem ser distribuídas) e a título do quê existe o fluxo. Ver Nissenbaum, 2010.

25 Em países de tradição democrática em geral não se viu empresas sendo forçadas a cederem bases de dados. Na Holanda, com forte tradição de proteção de dados, medida bastante semelhante ao SIMI que seria imposta forçadamente vem gerando críticas da autoridade competente de proteção de dados. Ver, por exemplo, "Privacy Watchdog slams coronavirus phone data mapping plan", Dutch News, 3 de julho de 2020, disponível em: https://www.dutchnews.nl/news/2020/07/privacy-watchdog-slams-coronavirus-phone-data-mapping-plan/.

26 No caso de muitos debates tidos no Brasil, mas principalmente ao redor do mundo quanto à criação e uso de aplicativos de *notificação de exposição* (inicialmente também chamado de "rastreamento de contatos"), pontuou-se que de nada valeria se não houvessem testes à disposição de pessoas para que pudessem confirmar diagnóstico sobre contaminação.

27 Para outros princípios que devem nortear o Poder Público ao avaliar soluções que envolvem uso de dados no combate à pandemia, e resguardado o entendimento exposto no artigo sobre a importância do princípio da legalidade, ver Bioni, Zanatta, Monteiro & Rielli, 2020.