O TRATAMENTO DE DADOS NO COMBATE À COVID-19: DILEMAS ENTRE O INTERESSE PÚBLICO E O DIREITO À PRIVACIDADE NA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS*

Gabriela Buarque Pereira Silva[1]

Jessica Andrade Modesto[2]

Marcos Ehrhardt Júnior[3]

Resumo: Desde o final de 2019, a pandemia da COVID-19 vem infectando e provocando a morte de milhares de pessoas em todo o mundo. Com a disseminação massiva da doença, diversos países têm adotado medidas de contenção, muitas das quais envolvem o tratamento de dados pessoais no intuito de mapear possíveis infectados, bem como identificar aqueles que não estão cumprindo o período de quarentena. Nesse panorama, o presente trabalho visa, por meio de método dedutivo de revisão bibliográfica e documental em doutrina, matérias jornalísticas e

* Esse texto é uma versão revisada do artigo "O tratamento de dados pessoais no combate à COVID-19: entre soluções e danos colaterais", o qual integra a coletânea: EHRHARDT JÚNIOR, Marcos; CATALAN, Marcos; MALHEIROS, Pablo. *Direito Civil e Tecnologia.* Belo Horizonte/MG: Editora Fórum, 2020 [livro digital].

[1] Mestranda em Direito Público pela Universidade Federal de Alagoas. Assessora Judiciária no TJ/AL.

[2] Mestranda em Direito Público pela Universidade Federal de Alagoas. Advogada. Servidora Pública Federal.

[3] Doutor em Direito pela Universidade Federal de Pernambuco (UFPE). Professor de Direito Civil da Universidade Federal de Alagoas (UFAL) e do Centro Universitário CESMAC. Editor da Revista Fórum de Direito Civil (RFDC). Vice-Presidente do Instituto Brasileiro de Direito Civil (IBDCIVIL). Presidente da Comissão de Enunciados do Instituto Brasileiro de Direito de Família (IBDFAM). Associado do Instituto Brasileiro de Estudos em Responsabilidade Civil (IBERC) e Membro Fundador do Instituto Brasileiro de Direito Contratual – IBDCont. Advogado.

legislação nacional e estrangeira, investigar possíveis danos derivados de tais medidas e a sua relação com o marco regulatório da Lei Geral de Proteção de Dados brasileira. Desse modo, constatou-se que, para evitar excessos antidemocráticos, o respeito à privacidade deve conviver com as medidas de tratamento de dados pessoais empregadas para o controle da pandemia, observando as diretrizes consagradas no ordenamento. As disposições da LGPD e a atuação da Autoridade Nacional de Proteção de Dados Pessoais demonstraram-se essenciais para garantir tal equilíbrio.

Palavras-Chave: Privacidade. Proteção de dados. Pandemia. Danos colaterais. Lei Geral de Proteção de Dados Pessoais.

DATA PROCESSING IN THE FIGHT AGAINST COVID-19: DILEMMS BETWEEN PUBLIC INTEREST AND THE RIGHT TO PRIVACY IN THE GENERAL PERSONAL DATA PROTECTION LAW

Abstract: Since the end of 2019, COVID-19 pandemic has been infecting and killing thousands of people around the world. With the massive spread of the disease, several countries have adopted containment measures, many of which involve the processing of personal data in order to map people possibly infected, as well as to identify those who are not complying with the quarantine period. In this context, the present work aims, through deductive method of bibliographic and documentary review of doctrine, journalistic articles and national and foreign statutes, to investigate possible damages derived from such measures and its relationships with the regulatory framework of the Brazilian General Law for Data Protection. Thus, it was found that, in order to avoid anti-democratic excesses, the respect for privacy must coexist with the personal data treatment measures employed to control the pandemic, observing the guidelines imposed in our

legal order. In this context, the provisions of the LGPD and the work of the National Personal Data Protection Authority have proved to be essential to ensure such a balance.

Keywords: Privacy. Data protection. Pandemic. Collateral damages. General Law on Protection of Personal Data.

1 INTRODUÇÃO

o final de 2019, a Organização Mundial da Saúde (OMS) recebeu um comunicado do governo chinês alertando sobre uma série de casos de pneumonia na província de Wuhan, cuja origem era, ainda, desconhecida. Em 9 de janeiro de 2020, foram anunciadas as primeiras análises sequenciais do vírus, as quais indicavam que a origem desses casos de pneumonia se devia a um novo tipo de coronavírus, que recebeu o nome técnico COVID-19 (ALVES, 2020).

Desde então, e até o momento de elaboração desse trabalho, a COVID-19 já matou mais de 1 milhão de pessoas e infectou mais de 40 milhões de indivíduos em todo o mundo (ECDC, 2020), o que fez com que, em 11 de março deste ano, a OMS declarasse a pandemia do coronavírus (MOREIRA; PINHEIRO, 2020). Também no Brasil, já se acumulam mais de 150 mil óbitos em razão da patologia, bem como mais de 5 milhões de infectados, conforme dados atualizados extraídos do sítio eletrônico do Ministério da Saúde (BRASIL, 2020a).

Toda essa situação tem feito com que os países adotem diversas medidas para a contenção da COVID-19, inclusive impondo às pessoas regimes de distanciamento social, a chamada quarentena. Nesse cenário, o tratamento de dados pessoais tem sido amplamente utilizado por diversos países no enfrentamento à pandemia.

Dados pessoais, para os fins deste trabalho, devem ser

compreendidos como informações relacionadas a uma pessoa identificada ou identificável, como o nome, o CPF, o endereço, os dados genéticos, o histórico médico, o *Internet Protocol* (IP) e os dados de localização de uma pessoa. São dados vinculados direta ou indiretamente a determinado indivíduo, os quais revelam algo sobre ele.

O tratamento dessas informações pode se mostrar bastante útil na execução de políticas governamentais de combate ao coronavírus. Isso porque os dados pessoais podem indicar as pessoas com quem o infectado teve contato e, assim, o governo pode contatá-las para que realizem testes de diagnóstico da COVID-19 e para que se mantenham em isolamento. Também é possível inferir, a partir da manipulação de tais dados, se as pessoas estão desrespeitando o período de quarentena, o que possibilita a adoção de medidas que garantam a efetividade dos decretos governamentais que obrigam ao distanciamento social.

Esses são só alguns exemplos de como os dados pessoais podem ser utilizados com vistas a se combater a COVID-19. As possibilidades são várias, no entanto, o uso indiscriminado de tais informações também pode gerar diversos danos colaterais. O presente trabalho se propõe a analisar, por meio de metodologia dedutiva, e como objetivo geral, as questões jurídicas que envolvem o tratamento de informações pessoais pelo poder público no enfrentamento à pandemia, bem como a abordar a necessidade de implementação da Lei Geral de Proteção de Dados Pessoais e da atuação da Autoridade Nacional para tutelar o direito à privacidade em meio à pandemia.

Nesse cenário, a título de objetivos específicos, busca-se responder aos seguintes questionamentos: o interesse coletivo pode justificar toda e qualquer limitação ao direito à privacidade ou há limites ao tratamento e divulgação desses dados em situações como a atual? O indivíduo pode sofrer danos colaterais decorrentes do tratamento de dados pessoais com vistas a combater a COVID-19? Como legislações específicas sobre a proteção de

dados pessoais podem resguardar os direitos dos titulares dos dados mesmo em momentos de crise?

Para tanto, procedeu-se a uma pesquisa bibliográfica/documental acerca do tema em doutrina, matérias jornalísticas e legislação nacional e estrangeira, com vistas a identificar quais são as medidas de enfrentamento à pandemia que utilizam dados pessoais adotadas pelo Brasil e demais Estados, quais os potenciais danos que essas medidas podem acarretar, bem como qual a importância da Lei Geral de Proteção de Dados Pessoais para regular a referida utilização das informações pessoais.

2 UTILIZAÇÃO DE DADOS PESSOAIS NO COMBATE À COVID-19: ENTRE SOLUÇÕES E DANOS COLATERAIS

Do intenso noticiário a respeito do combate à pandemia, é possível extrair algumas informações relevantes. Cingapura emitiu diretrizes consultivas esclarecendo que os dados pessoais podem ser coletados, usados ou divulgados, sem o consentimento, para fins de proteção de saúde dos habitantes, rastreamento de contatos e outras medidas de resposta.

Na Itália, um decreto-lei, emitido em 9 de março de 2020, autorizou o compartilhamento de dados entre as autoridades de saúde e a comunidade civil para gerenciar a emergência.

A inteligência artificial também vem rastreando padrões espaciais da patologia. Uma empresa canadense chamada *BlueDot* coleta dados multilíngues de bases de dados oficiais da saúde pública para prever potenciais surtos (WIRED, 2020).

Pesquisadores da *Harvard Medical School* coletam dados autorizados e dados de mídias sociais para explorar tendências geográficas da doença (WIRED, 2020).

Na China, drones já estão sendo utilizados para alertar a população a usar máscaras (GLOBAL NEWS, 2020); placas e tecnologias de reconhecimento fácil vêm rastreando pessoas e pedindo que se mantenham em isolamento (REUTERS, 2020),

além da implantação de *scanners* infravermelhos em estações de trem e aeroportos, que detectam indivíduos com febre (SOUTH CHINA MORNING POST, 2020). A China também implementou um aplicativo que classifica as pessoas segundo riscos de contágio e determina quem deve ficar em quarentena, além de enviar dados à polícia chinesa (THE NEW YORK TIMES, 2020). A empresa responsável pelo aplicativo e as autoridades não explicam como exatamente o sistema funciona, não sendo possível, no momento, avaliar com mais profundidade a dinâmica de utilização dos dados pessoais naquele país, que nos últimos anos vem se destacando na utilização de ferramentas de tratamento de dados biométricos para as mais diversas finalidades, em geral, estabelecidas e controladas pelo governo central[4].

Em Taiwan e Israel, *smartphones* foram programados para notificar as autoridades públicas caso os pacientes não observem a quarentena (THE TELEGRAPH, 2020 e DATA GUIDANCE, 2020), em um sistema de rastreamento.

Na Coreia do Sul, foram divulgados os dados de viagens

[4] Neste ponto, interessante destacar matéria publicada no jornal El País, com o seguinte título "*O coronavírus de hoje e o mundo de amanhã, segundo o filósofo Byung-Chul Han*", que compara o modo ocidental de se comportar perante as mais diversas formas de vigilância digital com a perspectiva oriental: "(...) A consciência crítica diante da vigilância digital é praticamente inexistente na Ásia. Já quase não se fala de proteção de dados, incluindo Estados liberais como o Japão e a Coreia. Ninguém se irrita pelo frenesi das autoridades em recopilar dados. Enquanto isso a China introduziu um sistema de crédito social inimaginável aos europeus, que permite uma valorização e avaliação exaustiva das pessoas. Cada um deve ser avaliado em consequência de sua conduta social. Na China não há nenhum momento da vida cotidiana que não esteja submetido à observação. Cada clique, cada compra, cada contato, cada atividade nas redes sociais são controlados. Quem atravessa no sinal vermelho, quem tem contato com críticos do regime e quem coloca comentários críticos nas redes sociais perde pontos. A vida, então, pode chegar a se tornar muito perigosa. Pelo contrário, quem compra pela Internet alimentos saudáveis e lê jornais que apoiam o regime ganha pontos. Quem tem pontuação suficiente obtém um visto de viagem e créditos baratos. Pelo contrário, quem cai abaixo de um determinado número de pontos pode perder seu trabalho. Na China essa vigilância social é possível porque ocorre uma irrestrita troca de dados entre os fornecedores da Internet e de telefonia celular e as autoridades. Praticamente não existe a proteção de dados. No vocabulário dos chineses, não há o termo "esfera privada". (EL PAÍS, 2020).

de 29 pacientes confirmados, compilados por meio de bases de celulares, cartões de crédito e câmeras de segurança (DAILY MAIL, 2020).

Nessa breve digressão, é possível perceber que o tratamento dos dados pessoais está sendo utilizado para geolocalização, identificação e rastreamento de pacientes, gerenciamento do risco de contágio, entre outras atividades, com a finalidade de melhorar os instrumentos de combate à pandemia.

Não se pode ignorar que o tratamento de dados pessoais é uma importante ferramenta nessa luta. No entanto, esse tratamento deve ser feito de maneira proporcional ao fim almejado, não se admitindo que uma quantidade excessiva de informações pessoais seja coletada, e muito menos exposta, sob pena de ofensa ao direito fundamental à privacidade. Isso porque, se os dados não forem utilizados de maneira necessária, adequada e adstrita às finalidades para as quais foram coletados, esse tratamento pode gerar diversos danos colaterais.

No Brasil, por exemplo, após viajar para o casamento de um amigo, no início do mês de março, C. R. desembarcou no aeroporto da capital sergipana. Alguns dias depois, começou a sentir uma dor de cabeça, que logo evoluiu para sintomas que ela acreditou serem de uma gripe e que a deixaram indisposta. Foi quando recebeu uma ligação da Vigilância Epidemiológica de Aracaju, a informar que o órgão estava buscando as pessoas que estiveram no mesmo voo que C.R., porque um dos passageiros fora diagnosticado com coronavírus. A vigilância solicitou, então, que C.R. fosse a um hospital para realizar um exame para o diagnóstico da COVID-19 (G1, 2020).

Antes mesmo de saber do resultado do teste, que deu positivo para o coronavírus, os dados pessoais de C.R. já estavam circulando nas redes sociais. Juntamente com seu nome, foto e local de trabalho, as pessoas compartilhavam em tais redes diversos ataques a ela, os quais iam desde inverdades a respeito do descumprimento do isolamento até afirmações de que ela

merecia ser presa. Tudo isso fez C.R. afirmar que a exposição que sofreu a deixou mais doente do que o próprio coronavírus.

Na Coreia do Sul, "S" participa de uma aula, em seu trabalho, sobre assédio sexual. Acaba contraindo o coronavírus em decorrência do instrutor da turma. Assim que é diagnosticado com a doença, o governo começa a enviar mensagens para a população informando sobre o diagnóstico. Nas mensagens constam o sexo, a idade, o distrito de residência e o distrito de trabalho do infectado, a ocasião e de quem o infectado contraiu o vírus, os locais e horários por onde passou após a infecção e, até mesmo, a informação de que "S" e o instrutor estiveram juntos em um bar até as 23h03, o que gerou boatos de que os dois teriam um romance. Apesar de nenhum nome ou endereço ser informado, não é difícil imaginar como a divulgação dessa vasta quantidade de dados, a princípio não identificados, torna-os facilmente identificáveis (BBC NEWS, 2020).

Ainda na Coreia do Sul, outro alerta no celular informa que uma mulher de 27 anos que trabalha na Samsung, em Gumi, contraiu a COVID-19 no dia 18 de fevereiro, às 23h, quando visitou sua amiga que havia participado da reunião da seita religiosa Shincheonji, a maior fonte de infecções no país. Logo depois, o prefeito de Gumi revelou o sobrenome da coreana em seu Facebook, momento em que os moradores da cidade, em pânico, começaram a pedir que o prefeito lhes dissesse o endereço da infectada. Assustada, a mulher implorou por meio da rede social que o prefeito não divulgasse suas informações pessoais, pois tal comportamento poderia trazer danos à família dela e a seus amigos, o que, para a infectada, era mais difícil que a dor física.

Não à toa, em 14 de março, o Centro de Controle e Prevenção de Doenças (*Korea Centers for Disease Control and Prevention – KCDC),* divulgou diretrizes para a coleta e divulgação de dados, determinando que os contatos a serem rastreados devem ser determinados com base nos sintomas e condições de exposição do paciente e vedando a divulgação de informações

pessoais (YONHAP NEWS AGENCY, 2020).

Toda essa riqueza de informações que o governo divulga em seus alertas é fruto de uma massiva coleta dos dados pessoais daqueles que são infectados pelo coronavírus, que vai da entrevista do paciente até a verificação das transações com cartões de crédito feitas pelo infectado, passando pela coleta de dados de localização dos *smartphones* e filmagens de câmeras de vigilância para recriar a rota do infectado um dia antes de os sintomas aparecerem.

Diante de tantos casos em que a identificação dos infectados foi possível, situações de linchamento virtual, além de casos que, mesmo não havendo a identificação, geraram diversos comentários vexatórios, os sul-coreanos passaram a ter tanto ou até mais medo do estigma social, das críticas e de outros danos do que da própria doença. Ademais, os alertas também estão afetando lojas e restaurantes, já que as mensagens associam os nomes desses estabelecimentos ao vírus. Esse fato tem sido utilizado por pessoas mal-intencionadas que contraíram o coronavírus e passaram a chantagear os proprietários de tais estabelecimentos, exigindo dinheiro em troca de não informarem às autoridades de saúde que por lá passaram (KIM, 2020).

Nesse cenário, surgem alguns questionamentos: os Estados podem coletar e tratar nossos dados pessoais para combater a pandemia, sem aviso prévio e informação sobre a natureza e a extensão dos dados coletados? O interesse coletivo pode justificar toda e qualquer limitação ao direito à privacidade? Há limites ao tratamento e à divulgação de dados pessoais realizados pelos Estados em situações como essas?

Na atualidade, o direito à privacidade tem sua compreensão ampliada em razão de a evolução das formas de divulgação e a apreensão de dados pessoais terem expandido as possibilidades de violação da esfera privada, máxime pelo acesso não autorizado de terceiros a esses dados.

Nesse sentido, Anderson Schreiber (2014, p. 137) afirma

que, numa "sociedade caracterizada pelo constante intercâmbio de informações, o direito à privacidade deve se propor a algo mais que àquela finalidade inicial, restrita à proteção da vida íntima", devendo abarcar também o direito do indivíduo de manter o controle sobre seus dados pessoais.

Dessa feita, a tutela da privacidade alarga seus contornos tradicionais de "direito a ser deixado só" ou "direito de ser deixado em paz" (BRANDEIS, WARREN, 1890), para apresentar-se também como o direito de manter o controle sobre as próprias informações e de determinar as modalidades de construção da própria esfera privada (RODOTÁ, 2008, p. 109).

Nesse contexto, o direito à proteção de dados pessoais é reconhecido como uma espécie do direito fundamental à privacidade (PEIXOTO; EHRHARDT JÚNIOR, 2018) e alicerça-se na autodeterminação informativa, isto é, sinteticamente, no direito de cada indivíduo decidir quando e como dispor de suas informações.

Como já mencionado, o conceito de dado pessoal pode ser entendido como os fatos, comunicações e ações que se referem a um indivíduo identificado ou identificável (MENDES, 2014, p. 55-56). Em outras palavras, dado pessoal é todo dado relacionado a uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como, por exemplo, um nome, um número de identificação, dados de localização, identificadores por via eletrônica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, econômica, cultural ou social dessa pessoa singular (MENDES, 2014, p. 55-56).

A proteção aos dados pessoais é um direito fundamental, devendo, portanto, ser assegurado pelo Estado. Entretanto, nas situações concretas, seja nas relações particulares, seja nas relações entre indivíduo e Estado, muitas vezes a coexistência equilibrada dos direitos fundamentais de diferentes titulares não é tarefa fácil, de modo que a realização plena e simultânea desses

direitos nem sempre é possível.

Com efeito, trata-se, assim, de um aparente choque entre o interesse público e o direito à privacidade. Nesse contexto, compete evidenciar que o dito princípio da supremacia do interesse público sobre o interesse privado passa por revisitações que modificam a clássica ideia de sobreposição entre um e outro, abrindo espaço para margens de ponderação e proporcionalidade. A definição de interesse público, então, e de sua propalada supremacia sobre os interesses particulares, deixa de estar ao inteiro arbítrio do administrador, passando a depender de juízos de ponderação proporcional entre os direitos fundamentais e outros valores e interesses metaindividuais constitucionalmente consagrados (BINENBOJM, 2005, p. 8).

Segundo a doutrina especializada, essas situações devem ser solucionadas por meio da ponderação (ALEXY, 1999), isto é, balanceando-se os bens em jogo, conforme as circunstâncias fáticas do caso concreto (LINHARES, 2001), na busca de se chegar à solução em que todos os direitos envolvidos tenham a máxima efetividade possível de acordo com tais circunstâncias.

No mesmo trilhar, a rejeição das especificidades de cada caso, impondo uma única e invariável relação de prevalência do interesse público, termina por distanciar-se do princípio da proporcionalidade, mormente no que tange às suas acepções – adequação (o meio escolhido deve ser o apto a atingir o fim a que se destina), necessidade (dentre os meios hábeis, a opção deve incidir sobre o menos gravoso em relação aos bens envolvidos) e proporcionalidade em sentido estrito (a escolha deve trazer maiores benefícios do que a restrição proporcionada) (BINENBOJM, 2005, p. 17).

Por óbvio, não é a primeira vez que situações como essa surgem no campo jurídico. A título de exemplo, não se confunde a questão da utilização de dados sensíveis em desconformidade com a LGPD com a divulgação de dados referentes à remuneração de servidores em cargos públicos, uma vez que tais

informações são atinentes ao cargo e há interesse público nessa transparência[5]. Em sentido análogo, também se entende que o sigilo bancário deve ceder em situações específicas, com observância do procedimento legal e com respeito ao princípio da razoabilidade[6]Isso porque não há, no ordenamento jurídico brasilero, direitos que se revistam de caráter absoluto, de modo que relevantes razões de interesse público podem, em determinadas circunstâncias, ainda que de forma excepcional, ensejar a adoção de algumas medidas restritivas, desde que respeitados parâmetros mínimos que permitam a convivência com o regime das liberdades e direitos fundamentais.

---

[5] AGRAVO REGIMENTAL NO RECURSO EXTRAORDINÁRIO. CONSTITUCIONAL. PRINCÍPIOS DA PUBLICIDADE E DA TRANSPARÊNCIA. AUSÊNCIA DE VIOLAÇÃO À INTIMIDADE E À PRIVACIDADE. DISTINÇÃO ENTRE A DIVULGAÇÃO DE DADOS REFERENTES A CARGOS PÚBLICOS E INFORMAÇÕES DE NATUREZA PESSOAL. OS DADOS PÚBLICOS SE SUBMETEM, EM REGRA, AO DIREITO FUNDAMENTAL DE ACESSO À INFORMAÇÃO. DISCIPLINA DA FORMA DE DIVULGAÇÃO, NOS TERMOS DA LEI. PODER REGULAMENTAR DA ADMINISTRAÇÃO. AGRAVO REGIMENTAL A QUE SE NEGA PROVIMENTO. I – O interesse público deve prevalecer na aplicação dos Princípios da Publicidade e Transparência, ressalvadas as hipóteses legais. *II – A divulgação de dados referentes aos cargos públicos não viola a intimidade e a privacidade, que devem ser observadas na proteção de dados de natureza pessoal*. III – Não extrapola o poder regulamentar da Administração a edição de portaria ou resolução que apenas discipline a forma de divulgação de informação que interessa à coletividade, com base em princípios constitucionais e na legislação de regência. IV – Agravo regimental a que se nega provimento. (RE 766390 AgR, Relator(a): RICARDO LEWANDOWSKI, Segunda Turma, julgado em 24/06/2014, PROCESSO ELETRÔNICO DJe-157 DIVULG 14- 08-2014 PUBLIC 15-08-2014.

[6] AGRAVO REGIMENTAL NO AGRAVO DE INSTRUMENTO. MATÉRIA INFRACONSTITUCIONAL. SIGILO BANCÁRIO. QUEBRA. PROCEDIMENTO LEGAL. OFENSA INDIRETA À CONSTITUIÇÃO DO BRASIL. 1. Controvérsia decidida à luz de normas infraconstitucionais. Ofensa indireta à Constituição do Brasil. *2. O sigilo bancário, espécie de direito à privacidade protegido pela Constituição de 1988, não é absoluto, pois deve ceder diante dos interesses público, social e da Justiça. Assim, deve ceder também na forma e com observância de procedimento legal e com respeito ao princípio da razoabilidade.* Precedentes. 3. Agravo regimental a que se nega provimento. (AI 655298 AgR, Relator(a): EROS GRAU, Segunda Turma, julgado em 04/09/2007, DJe-112 DIVULG 27-09-2007 PUBLIC 28-09-2007 DJ 28-09-2007 PP-00057 EMENT VOL-02291-13 PP-02513 RNDJ v. 8, n. 95, 2007, p. 87-88)

Assim, situações como a atual pandemia podem envolver conflitos entre diferentes direitos fundamentais, que, no caso, se consubstanciam entre o embate entre o direito de privacidade e o direito à saúde, também estipulado no art. 196 da Constituição Federal como direito de todos e dever do Estado, garantido mediante políticas sociais e econômicas que visem à redução do risco de doença e de outros agravos. Quando isso acontece, é preciso buscar soluções jurídicas que permitam que todos os direitos sejam, em algum grau, resguardados.

Desse modo, se o tratamento de dados pessoais se mostrar uma medida adequada e necessária ao combate da pandemia, de modo a resguardar o direito à vida e à saúde de toda a coletividade, o Estado poderá, sim, restringir parcialmente a privacidade, assim como o faz, com as determinações de distanciamento social, com outros direitos, a exemplo do direito de associação, que é temporariamente obstaculizado visando impedir a disseminação da COVID-19.

No que diz respeito ao tratamento de dados pessoais para esse fim, a existência ou não de legislação específica sobre a matéria no país muito influenciará a forma como isso ocorrerá, já que não há uma diretriz internacional única a ser seguida indistintamente por todos os Estados. Os diferentes ordenamentos jurídicos são mais ou menos permissivos quanto às hipóteses em que os dados pessoais podem ser legalmente tratados, bem como quanto aos princípios que tal tratamento deve seguir.

Antes de prosseguir na análise, é preciso estabelecer uma premissa fundamental: a proteção de dados e a utilização do seu tratamento para fins de proteção sanitária para a coletividade não são inteiramente incompatíveis, nem precisam ser consideradas sob uma lógica de exclusão (perde *x* ganha), pois podem coexistir, desde que observados certos princípios que necessitam de densificação à luz do caso concreto.

Na já citada Coreia do Sul, por exemplo, após o surto de Mers – uma epidemia asiática de outro coronavírus, em 2015, na

qual esse país foi o segundo com maior número de casos da doença –, o governo foi bastante censurado por ocultar informações que, na visão dos críticos, teriam ajudado a conter a disseminação, como dados sobre a localização dos pacientes.

Diante disso, aquele país promoveu mudanças significativas em sua legislação acerca do gerenciamento e compartilhamento público de informações sobre pacientes de doenças infecciosas. A *Personal Information Protection Act*, de 2016, passou a prever que as disposições legais que se referem ao consentimento, às limitações, bem como às garantias dos direitos dos titulares dos dados pessoais que devem ser observadas quando do tratamento de tais dados, não se aplicam às informações pessoais processadas temporariamente, quando urgentemente necessárias para a segurança, o bem-estar e a saúde pública (COREIA DO SUL, 2020).

Assim, possibilitou-se, em situações como a da COVID-19, uma vasta coleta de dados pessoais e a divulgação de uma quantidade considerável de dados não identificados, mas que, pela possibilidade de agregação, acabam por se tornar potencialmente identificáveis, o que tem gerado muitos problemas e discussões, mesmo em meio a toda a preocupação com a atual pandemia do coronavírus.

Para os que estão isolados e com receio de contrair a doença, a preocupação com a forma como ocorrerá o tratamento dos dados pessoais e eventuais abusos ao direito de privacidade parece ser uma questão de menor importância. No entanto, a experiência em outros países demonstra que a perspectiva muda radicalmente quando, uma vez infectada, a mesma pessoa passa a vivenciar as restrições provocadas pela exposição, muitas vezes não consentida nem sequer comunicada, de dados pessoais, incluindo dados sensíveis. Situações de discriminação e exclusão social nesses casos não têm uma duração que corresponda ao período da doença, podendo persistir por períodos muito mais longos.No Brasil, a vigência da Lei 13.709/2018 (Lei Geral de

Proteção de Dados – LGPD) se iniciou em setembro de 2020, remanescendo as sanções e penalidades em *vacatio legis* até agosto de 2021. Nesse contexto de pandemia e de intensa utilização de dados pessoais, não somente a vigência da LGPD, mas, principalmente, sua efetivação, são de suma relevância.

3 MEDIDAS DE ENFRENTAMENTO À PANDEMIA E A IMPORTÂNCIA DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

A Lei 13.709/2018, nossa primeira lei geral sobre proteção de dados pessoais, visa regular o tratamento das informações pessoais pelos setores públicos e privados. Ressalte-se que, em abril de 2016, o Parlamento Europeu adotou o Regulamento Geral de Proteção de Dados (GDPR), que entrou em vigor em 2018 e substituiu a Diretiva de Proteção de Dados da União Europeia de 1995, regulando a temática da proteção de dados pessoais nos países envolvidos de modo vinculante.

O GDPR é um regulamento pelo qual o Parlamento Europeu, o Conselho da União Europeia e a Comissão Europeia objetivam reforçar e unificar a proteção dos dados pessoais para todos os indivíduos da União Europeia, harmonizando as leis de privacidade de dados em toda a Europa (MAGRANI, 2019, p. 102).

Os princípios do GDPR e da Lei 13.709/18 (Lei Geral de Proteção de Dados – LGPD) são extremamente semelhantes e partem do pressuposto de tutela da privacidade numa sociedade democrática (MAGRANI, 2019, p. 103). A LGPD importa a essência dos princípios do GDPR, tornando-se evidente a inspiração europeia na formulação do diploma legislativo brasileiro. A LGPD, no art. 6º, traz como princípios a finalidade, a adequação, a necessidade, o livre acesso, a qualidade dos dados, a transparência, a segurança, a não discriminação, a responsabilização e a prestação de contas. Além desses princípios, o GDPR

menciona expressamente, em seu art. 6º, a licitude, a lealdade, a limitação da conservação, a integridade e a confidencialidade.

Em que pesem tais sutis diferenças, ambos os diplomas normativos são aplicáveis às entidades públicas e privadas que tratam os dados pessoais, prevendo direitos atribuíveis aos titulares cujos dados são processados, disciplinam obrigações aos agentes de tratamento e estabelecem sanções em face do descumprimento.

O documento assume relevância tendo em vista que os dados são o efetivo combustível da inteligência artificial, caracterizando o que se chama de *Big Data.* A expressão pode ser conceituada como um grande conjunto de dados, cada vez mais alimentado graças à presença de dispositivos sensores na vida cotidiana e ao crescente número de indivíduos conectados a essas tecnologias por meio de redes digitais (ITS RIO, 2019).

No Brasil, a LGPD, em seu artigo 11, determina que o tratamento de dados pessoais sensíveis, aí incluídos os dados referentes à saúde, somente poderá ocorrer quando o titular consentir, de forma expressa e destacada, para finalidades bem específicas.

Na sequência, são disciplinadas situações em que o tratamento dos dados sensíveis poderá ocorrer sem o consentimento do seu titular, tais como quando for indispensável ao cumprimento de obrigação legal ou regulatória, à execução de políticas públicas, à realização de estudos por órgão de pesquisa, à proteção da vida ou da incolumidade física do titular ou de terceiro e à garantia da prevenção à fraude e à segurança do titular, entre outras.

No ponto que interessa à nossa reflexão, a LGPD também eximirá a necessidade do prévio consentimento quando estiver em evidência a tutela da saúde, exclusivamente em procedimento realizado por profissionais da área, serviços de saúde ou autoridade sanitária. Isso não quer dizer que as outras previsões legais da Lei 13.709/2018 não são aplicáveis ao tratamento

de dados realizados nas referidas hipóteses.

Ao contrário, os direitos dos titulares continuam garantidos, assim como também devem ser observados os princípios elencados no artigo 6º da referida lei. Esses princípios são reconhecidos internacionalmente como essenciais às liberdades fundamentais dos titulares dos dados e, por conta disso, são observados pela legislação de proteção de dados de muitos países, e até mesmo reconhecidos doutrinária e jurisprudencialmente em países que não contam com legislação específica acerca da matéria.

Dito isso, qualquer atividade de tratamento de dados pessoais deverá observar a *boa-fé objetiva* e a *finalidade* do tratamento, vale dizer, sua realização, propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades. Apenas a finalidade não é suficiente. É preciso compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento, o que impõe a exigência de *adequação*.

Mesmo com tratamento adequado e existindo propósitos legítimos, ainda resta avaliar a *necessidade* do tratamento, que deve se limitar ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos. Considerando os dados pessoais como extensão dos direitos de personalidade da pessoa natural, devem-se garantir aos titulares dos dados informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento (responsáveis pela coleta e utilização dos dados), como expressão da *transparência* que deve ser mantida em operações desse tipo.

Não se pode transigir quanto à impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos. A lógica da *não discriminação* é inegociável e deve vir acompanhada da necessária *responsabilização* e *prestação de*

contas, que ocorre com a demonstração, por parte do agente responsável pelo tratamento, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais, e a eficácia dessas medidas, a fim de prevenir a ocorrência de danos, em especial aqueles decorrentes de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão de informações pessoais.

Assim, mesmo em meio a uma pandemia como a COVID-19, deve-se tutelar a privacidade, ainda que esta seja submetida a algumas restrições que o momento exige. Desse modo, ao tomar determinada medida que se utilize do tratamento de dados pessoais no enfrentamento à transmissão do coronavírus, o Estado deve fazer um juízo de ponderação, bem como avaliar se a medida atende aos princípios de proteção de dados pessoais.

Nesse contexto, questiona-se se a coleta e a divulgação de tantos dados pessoais como tem ocorrido na Coreia do Sul é medida realmente necessária para o combate à pandemia. Sobre isso, pode-se argumentar que o país tornou-se exemplo no enfrentamento à COVID-19, conseguindo, em poucas semanas, fazer com que o número de casos confirmados por dia caísse dos três dígitos para algumas dezenas (MOREIRA, 2020). No entanto, até que ponto se pode atribuir tal feito à utilização das informações pessoais?

Além dos alertas sobre novos infectados, a Coreia do Sul tornou-se o país que mais seleciona pessoas *per capita* a fim de realizar o teste para diagnóstico do coronavírus no mundo, disponibilizando milhares de exames gratuitos ou a preços bastante acessíveis, no intento de alcançar a participação de grande parte da população. Os testes podem ser feitos por meio de *drive thru*. Ainda, pequenas e grandes organizações empresariais passaram, de forma voluntária, a cancelar reuniões e a incentivar o *home office*.

Apesar de não ser possível analisar, pelo menos no

momento, o grau de eficácia de cada uma das medidas adotadas, é certo que nenhuma delas, sozinha, foi a responsável pela acentuada queda no número de novas infecções.

Com tantas outras medidas sendo adotadas, a divulgação de tantos dados dos infectados não se mostrou excessiva e desproporcional à finalidade de alertar a outros sul-coreanos que estes poderiam ter sido contaminados? Tal divulgação, caso ocorresse de modo semelhante em nosso país, seria tratada como "mero aborrecimento" e não ensejaria a possibilidade de reparação? Ou seria possível vislumbrar os contornos do disposto no art. 187 do Código Civil, que veda o abuso do direito?

A divulgação pública de informações como a situação em que a pessoa contraiu o COVID-19, bem como de qual infectado contraiu o vírus, é realmente necessária para o combate da pandemia? Não bastaria que as autoridades de saúde tivessem o conhecimento da situação?

Não se pode ignorar que o tratamento de dados pessoais pode ser uma importante ferramenta no combate à pandemia. Localizar pessoas que estiveram em contato com indivíduos diagnosticados com a COVID-19 é medida importante, principalmente tendo em vista que muitos dos portadores do vírus são assintomáticos ou desenvolvem sintomas leves, facilmente confundidos com os de outras doenças, o que pode obstaculizar o diagnóstico e, por conseguinte, inviabilizar que o infectado tome as medidas adequadas para não transmitir o vírus a outras pessoas.

Entretanto, esse tratamento deve ser feito de maneira proporcional ao fim almejado, não se admitindo que uma quantidade excessiva de informações pessoais seja coletada, e muito menos exposta, sob pena de ofensa ao direito fundamental à privacidade, cuja eficácia não depende da, nem está condicionada à vigência da LGPD.

Por trazer uma série de princípios e diretrizes que devem ser observados quando do tratamento de dados, inclusive pelo

Poder Público, a Lei Geral de Proteção de Dados Pessoais consolida, em nosso ordenamento jurídico, os padrões de proteção aos dados pessoais reconhecidos internacionalmente, densificando a realização desse direito fundamental, o que possibilita uma maior uniformização na aplicação do direito à proteção de dados pessoais pelos setores público e privado, bem como pelo Judiciário e demais intérpretes do Direito.

Já a efetividade da LGPD demanda a atuação da Autoridade Nacional de Proteção de Dados. Não sem razão, dos mais de 120 países que aprovaram leis sobre a matéria, somente 12 não criaram uma autoridade independente (VASCONCELOS; PAULA, 2019, p. 722). Isso porque as leis não são autoimplementáveis, ao contrário, sua efetividade tem sido fortemente atrelada à existência e ao modo de atuação das autoridades de proteção de dados pessoais.

Diante disso, os países que não criam essas autoridades são criticados por aprovarem leis sem fornecer o mecanismo institucional por meio do qual a conformidade com a lei e as boas práticas serão incentivadas e fiscalizadas (RAAB; SKEZELY, 2020, p. 421).

As Autoridades de Proteção de Dados exercem várias funções, sendo as principais as de ouvidoria, auditoria, consultoria, educação, consultoria e políticas públicas, negociação e execução da legislação. Ressalte-se, contudo, que esse rol de atividades não é universalmente encontrado entre as competências de todas as autoridades, de modo que algumas delas podem enfatizar a aplicação da lei, outras podem se concentrar em educar o público, e as organizações podem estar mais envolvidas na orientação de políticas públicas e na elaboração de códigos de conduta (RAAB; SKEZELY, 2020, p. 422).

O Brasil seguiu a experiência internacional. Assim, competirá à Autoridade Nacional de Proteção de Dados não só garantir a aplicação da LGPD pelos agentes de tratamento, fiscalizando e aplicando sanções em caso de tratamento de dados

realizado em descumprimento à legislação, mas também promover o conhecimento da população acerca de seus direitos e da forma de exercê-los, além de efetivar mecanismos simplificados e virtuais para o registro de reclamações sobre o tratamento de dados pessoais em desconformidade com a lei.

Ademais, à ANPD caberá dispor sobre padrões técnicos mínimos de segurança dos dados, estimular a adoção de padrões técnicos que facilitem o controle pelos titulares dos seus dados pessoais, bem como reconhecer e divulgar regras de boas práticas e de governança adotadas pelos agentes de tratamento.

Ainda, compete-lhe realizar auditorias, deliberar em caráter terminativo, na esfera administrativa, sobre a interpretação da LGPD, além de editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade, bem como sobre relatórios de impacto à proteção de dados pessoais para os casos em que o tratamento representar alto risco à garantia dos princípios gerais de proteção de dados pessoais. Caberá à ANPD, também, regulamentar diversas disposições da lei.

Isso posto, é evidente a importância da Autoridade Nacional para a implementação da legislação sobre a proteção de dados. Sem esse órgão, mais que ficar incompleto, o sistema de proteção poderá se tornar ineficiente, causar insegurança jurídica e deixar nas mãos do Judiciário, já tão assoberbado e sem especialistas na matéria, a tarefa de dar concretude a muitas das previsões da Lei Geral de Proteção de Dados Pessoais, o que dificultará a manutenção de padrões no que concerne à aplicação da lei.

Não sem motivo, o veto da Lei 13.709/2018, que impediu a criação da Autoridade Nacional por questões técnicas, bem como o ínterim entre a aprovação da Medida Provisória 869/2018 que a criou e a sua conversão na referida lei, gerou grande preocupação entre os especialistas da área, que temiam a entrada em vigor da lei sem que a autoridade estivesse pronta para funcionar.

Como exemplo, no Peru, a Autoridade Nacional de Proteção de Dados Pessoais tem atuado bastante nessa pandemia. Elaborou um guia para estabelecimentos de saúde recomendando medidas para garantir a confidencialidade dos dados dos pacientes com COVID-19, as quais, se não adotadas, podem caracterizar uma infração grave sancionável com multa de até 215.000 soles, além de advertir que revelar dados de saúde sem o consentimento pode violar a esfera mais íntima da pessoa e gerar discriminação (MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS DE PERU , 2020).

A autoridade nacional peruana também tem orientado a mídia a só divulgar informações sobre o número de pacientes atendidos, idade, sexo, local de infecção, além de informações que não identifiquem ou tornem identificáveis os pacientes com COVID-19, ressaltando que a publicação de dados de saúde que identificam pessoas será considerada uma violação grave à Lei de Proteção de Dados Pessoais do país. Ainda, tem divulgado seu *e-mail* e contato telefônico para que os peruanos possam buscar informações acerca da proteção de seus dados (PERU, 2020).

Por fim, bastante relevante é o acompanhamento e a supervisão, pela Autoridade Nacional, da utilização dos dados obtidos em razão do Decreto peruano 070-2020-PCM, o qual estabelece que as entidades que administram as centrais telefônicas de emergência 113 (Ministério da Saúde) e 107 (ESSALUD) acessem os dados pessoais daqueles que fazem chamadas relatando sintomas do novo coronavírus. Essas informações deverão ser anonimizadas e enviadas às várias entidades para o cumprimento das funções e competências sob sua responsabilidade (PERU, 2020).

Assim, a referida autoridade assegura que os dados sejam utilizados apenas para os fins estabelecidos no decreto e que o tratamento seja realizado de acordo com a lei peruana de proteção de dados e os regulamentos da autoridade, atuando para que

as entidades que acessem esses dados estabeleçam medidas técnicas, organizacionais e legais correspondentes para salvaguardar a confidencialidade, a integridade e a disponibilidade dos dados até sua exclusão, após o término do Estado Nacional de Emergência.

A pandemia deixou bem evidente a necessidade da legislação específica sobre proteção de dados pessoais no Brasil. Nós já contamos com esse marco regulatório, que foi a aprovação da Lei 13.709/2018, a LGPD, contudo, faz-se imprescindível não só que entre em vigor, mas também que seja implementada, máxime com a atuação da Autoridade Nacional.

Entretanto, o que se viu durante essa crise foram várias tentativas de postergar a *vacatio legis* da Lei Geral de Proteção de Dados Pessoais. Embora a Autoridade Nacional tenha sido criada há mais de um ano, ainda não foi montada a estrutura para que venha a funcionar.

A Autoridade Nacional foi criada como órgão da administração pública federal direta, integrante da Presidência da República, prejudicando a existência de um mecanismo institucional verdadeiramente eficaz de fiscalização e aplicação da LGPD. Isso porque, para que a Autoridade Nacional possa exercer suas funções de maneira eficiente, faz-se necessário que ela seja independente, com real autonomia, na prática, para o desempenho de suas atividades, inclusive no que diz respeito ao setor público, que também é regulado pela LGPD.

Nesse diapasão, tem-se a previsão do artigo 55-A, da § 1º, da LGPD, que dispõe que a natureza jurídica da ANPD poderá ser transformada em entidade da administração pública federal indireta, submetida a regime autárquico especial, o que poderá ocorrer em até dois anos após a entrada em vigor da estrutura regimental da Autoridade Nacional. Aguarda-se que tal transformação aconteça, tendo em vista a essencialidade de sua independência. Demonstrada a necessidade da Lei Geral de Proteção de Dados Pessoais e da atuação da Autoridade Nacional,

cumpre investigar a utilização de dados pessoais no enfrentamento à COVID-19 enquanto estava pendente a vigência da LGPD.

4 O TRATAMENTO DE DADOS PESSOAIS PARA FINS DE PROTEÇÃO SANITÁRIA NO BRASIL DURANTE A *VACATIO LEGIS* DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

Em Recife, a prefeitura municipal começou a utilizar sistemas de localização de celulares dos recifenses para coordenar ações de incentivo ao isolamento social. Segundo a prefeitura, o tratamento de dados pessoais ocorre de maneira coletiva, para se verificar, bairro a bairro, se a orientação de isolamento domiciliar está sendo cumprida, o que permitirá a execução de uma série de ações para incentivar o isolamento social, como o envio de carros de som para a área, o envio de notificações por celular, além de outras ações de comunicação (G1, 2020).

Segundo informações divulgadas na imprensa, na iniciativa pernambucana observa-se a preocupação em não individualizar os dados tratados, já que isso não é necessário nem proporcional à finalidade buscada, que é a de se fazer uma análise, por área, a respeito de as pessoas estarem ou não saindo às ruas, e não a de se observar quem está fora de casa.

Ainda assim, mais transparência, com informações claras e em linguagem acessível sobre o modo de realização do tratamento de dados e o período de sua duração, seria bem-vinda, especialmente ante a impossibilidade de se poder contar com a fiscalização de uma Autoridade Nacional de Proteção de Dados.

No Amazonas, por exemplo, o governo estadual decretou regime de quarentena para os passageiros que desembarcarem no Aeroporto Internacional Eduardo Gomes. Além disso, o governo do Estado desenvolveu um aplicativo para *smartphones* que deverá ser instalado por todos esses passageiros e que

monitorará a localização, em tempo real, por 14 dias, das pessoas submetidas à quarentena (AMAZONAS, 2020).

Além de poder coletar e tratar dados pessoais sem o consentimento do indivíduo, o Estado pode, no combate à pandemia, obrigar o indivíduo a, de maneira ativa, fornecer tais dados, seja por meio de entrevista, seja por outro meio tecnológico?

No que diz respeito às medidas adotadas pelo governo federal, em fevereiro de 2020 foi publicada a Lei 13.979/20, que dispõe acerca de medidas para o enfrentamento da emergência de saúde pública de importância internacional, decorrente do coronavírus. Em seu art. 6º, o referido diploma legal dispõe 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, estendendo tal obrigação às pessoas jurídicas de direito privado quando os dados forem solicitados por autoridade sanitária.

Também dispõe que o Ministério da Saúde manterá dados públicos e atualizados sobre os casos confirmados, suspeitos e em investigação, relativos à emergência pública sanitária, resguardando o direito ao sigilo das informações pessoais. O art. 1º, nos parágrafos 2º e 3º, determina, ainda, que ato do ministro de Estado da Saúde disporá sobre a duração da emergência de saúde pública de que trata a lei, não podendo tal prazo ser superior ao declarado pela Organização Mundial de Saúde.

Nesse contexto, a Portaria 356/10 do Ministério da Saúde estipulou, em seu art. 12, que o encerramento da aplicação das medidas fica condicionado à avaliação de risco realizada pela Secretaria de Vigilância em Saúde do Ministério da Saúde sobre a situação de Emergência de Saúde Pública de Importância Nacional. Naturalmente, ainda não se sabe quanto tempo essa crise vai perdurar e, por conseguinte, por quanto tempo as medidas serão tomadas.

No que tange ao compartilhamento de dados, verifica-se que não há muita divergência em relação ao que prevê a LGPD, porquanto esta excepciona o acesso aos dados sensíveis, mesmo sem o consentimento, nos casos em que houver necessidade de tutela da saúde do titular ou de terceiros. Ademais, a nova legislação também dispõe que a utilização será restrita à finalidade de evitar a propagação do vírus e que, na hipótese de divulgação dos dados sobre casos confirmados, suspeitos e em investigação, será resguardado o direito ao sigilo das informações pessoais.

Da leitura dos dispositivos legais acima apontados, fica evidente que é indispensável compatibilizar a necessária proteção dos dados pessoais sensíveis, tais como informações relativas ao estado de saúde das pessoas, com o premente interesse público de adotar todas as medidas disponíveis para o combate da pandemia. Há de se prestigiar uma perspectiva de coexistência dos interesses em jogo e não de exclusão de qualquer dos polos da equação. Proteger o interesse coletivo não implica excluir a necessária proteção da pessoa natural, especialmente num estado de grave vulnerabilidade por esta acometida de uma nova doença ou pela mera suspeita de contágio, que já provoca abalos em seu bem-estar psíquico.

Diante de novos textos legislativos e de um contexto fático de crise que se altera muito rapidamente, ainda restam algumas preocupações a consignar. A Lei 13.979/20 determina que será obrigatório o compartilhamento de dados essenciais à identificação de pessoas infectadas ou com suspeita de infecção, sem elencar ou exemplificar que dados seriam esses, o que ocasiona insegurança jurídica em relação ao titular, que pode ter uma universalidade de dados pessoais compartilhados sem que sequer tenha ciência disso.

Com a vigência da Lei Geral de Proteção de Dados Pessoais, que se iniciou em setembro de 2020, as normas que têm emergido durante a pandemia passam a ter padrões mais objetivos no que diz respeito à proteção aos dados pessoais. É preciso

ressaltar, ainda, que o Brasil tem uma cultura de tutela de dados bem mais incipiente que diversos outros países, inclusive alguns de seus vizinhos, de modo que os princípios de proteção de dados pessoais internacionalmente reconhecidos são novidade para muitos integrantes dos três poderes.

Assim, em que pese a aplicação desses princípios não depender da LGPD, em um país no qual o direito à proteção de dados pessoais ainda tem um longo caminho a percorrer, uma legislação específica sobre o tema é essencial para que os intérpretes e aplicadores do Direito, a Administração Pública e os legisladores compreendam os interesses protegidos e as formas de realização desse direito, viabilizando, por conseguinte, que as normas voltadas ao enfrentamento da pandemia surjam em conformidade com a proteção da privacidade, ou seja, permitindo o tratamento de dados, mas respeitando os direitos dos titulares.

O funcionamento da ANPD, além de assegurar que somente sejam coletados os dados efetivamente necessários à finalidade pretendida, bem como que tais dados não sejam utilizados para fins outros, a Autoridade Nacional emitiria importantes regulamentos acerca do respeito aos direitos dos titulares e das medidas de segurança adequadas para o armazenamento dessas informações.

Ainda, importa dizer que o Marco Civil da Internet (Lei 12.965/2014) também é um instrumento de grande relevância na proteção dos direitos dos titulares dos dados no meio eletrônico. Isso porque a referida Lei buscou assegurar, de forma principiológica, os direitos e garantias do indivíduo, dentre os quais se encontra a proteção da privacidade e dos dados pessoais[7] (BIONI,

[7] [4] Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios:

I - garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal;

II - proteção da privacidade;

III - proteção dos dados pessoais, na forma da lei; IV - preservação e garantia da neutralidade de rede;

V - preservação da estabilidade, segurança e funcionalidade da rede, por meio de

2019, p. 130). Além disso, em seu artigo 7º, o MCI assegura ao indivíduo direitos como a inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação (I), bem como a inviolabilidade e o sigilo de comunicações pela internet (II) e das comunicações privadas armazenadas (III), exceto por ordem judicial.

Outrossim, o Marco Civil da Internet elege a autodeterminação informativa como parâmetro normativo para a proteção de dados pessoais, fazendo menção expressa à necessidade do consentimento do titular para a coleta, o armazenamento, o tratamento e o compartilhamento de seus dados pessoais com terceiros, bem como estabelecendo que tal consentimento seja livre, expresso e informado[8] (BIONI, 2019, p. 131-132).

Nesse contexto de incipiência, resta ao Judiciário fazer a ponderação entre tais normas e o direito à proteção de dados pessoais. Recentemente, o Supremo Tribunal Federal suspendeu a eficácia da Medida Provisória 954/2020, que prevê o compartilhamento de dados de usuários de telecomunicações com o Instituto Brasileiro de Geografia e Estatística (IBGE) para a produção de estatística oficial durante a pandemia da COVID-19

---

medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas;

VI - responsabilização dos agentes de acordo com suas atividades, nos termos da lei; VII - preservação da natureza participativa da rede;

VIII - liberdade dos modelos de negócios promovidos na internet, desde que não conflitem com os demais princípios estabelecidos nesta Lei.

Parágrafo único. Os princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte.

[8] Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos: [...] VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei; [...] IX - consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais; [...] Art. 16. Na provisão de aplicações de internet, onerosa ou gratuita, é vedada a guarda: I - dos registros de acesso a outras aplicações de internet sem que o titular dos dados tenha consentido previamente, respeitado o disposto no art. 7º ; [...]

(BRASIL, 2020b).

Para a ministra Rosa Weber, relatora das Ações Diretas de Inconstitucionalidade[9] que questionam a referida MP, os dados pessoais previstos na Medida Provisória integram o âmbito de proteção das cláusulas constitucionais que asseguram a liberdade individual, a privacidade e o livre desenvolvimento da personalidade, de modo que sua manipulação e seu tratamento devem observar os limites delineados pela proteção constitucional.

Diante disso, "ao não definir apropriadamente como e para que serão utilizados os dados coletados, a norma não oferece condições para a avaliação da sua adequação e necessidade". Ademais, entendeu a ministra que a medida provisória não apresenta mecanismo técnico ou administrativo para proteger os dados pessoais de acessos não autorizados, vazamentos acidentais ou utilização indevida, razão pela qual não satisfaz as exigências da Constituição em relação à efetiva proteção de direitos fundamentais.

Por fim, cumpre ressaltar que, além de esse controle judicial poder causar insegurança jurídica, verifica-se no contexto brasileiro a ausência de critérios de produção legislativa e uma crise política de gestão, o que torna ainda mais problemático o percurso da LGPD até a sua efetiva vigência.

CONCLUSÃO

No Brasil, a discussão sobre a privacidade ainda não chegou ao mesmo nível de profundidade dos outros países, tendo em vista que atualmente o aparato estatal não tem o mesmo grau de sofisticação para lograr objetivos massivos de vigilância.

Não se ignora que se trata de um processo desafiador. A admissão de tais medidas como ferramenta para o salvamento de vidas não pode ser afastada, máxime no panorama de extrema incerteza em que a pandemia se situa e do elevado número de

[9] ADI 6.387, ADI 6.388, ADI 6.389, ADI 6.390 e ADI 6.393.

mortes já ocasionadas em razão do vírus. Deixar as tecnologias que temos inutilizadas em face de uma situação de calamidade pública parece não fazer muito sentido.

O mais importante é que não nos esqueçamos de impor balizas a essas medidas, seja em termos de duração, seja em termos de supervisão legal e utilização de modo uniforme das informações coletadas, para que posteriormente tais dados não sejam utilizados com outros fins e a situação de emergência não nos faça recair em posterior excesso.

Torna-se crucial, então, definir parâmetros de transparência, principalmente quando da ocasião do envolvimento de empresas privadas do ramo tecnológico, que podem ver a oportunidade de, com espeque no argumento de eventuais avanços no combate ao vírus por meio do tratamento de dados, beneficiar-se nessa atividade num futuro próximo, sem possibilidade de se sindicar precisamente quais informações foram fornecidas durante o combate à pandemia.

A incógnita que se impõe é se as salvaguardas previstas na legislação atualmente em vigor, especialmente as leis e portarias criadas no momento da crise, serão suficientes para conter eventuais abusos que podem acontecer com o uso dos dados sensíveis num contexto de pós-pandemia.

Dados de localização, reconhecimento facial e rastreamento estão sendo utilizados como possíveis soluções para conter a difusão do vírus. O problema surge quando constatamos que, no meio de um cenário de tanto caos, é necessário parar para traçar fronteiras na utilização e no controle dessas ferramentas. O que será feito com esses dados após a contenção do surto? Medidas de vigilância realmente são eficazes para limitar a propagação da patologia? Os titulares terão ciência desse tratamento? Como será feita a custódia?

São questionamentos que inquietam e que ainda não têm uma resposta formulada, sobretudo em razão da priorização estatal na resolução da crise pandêmica e da ausência de uma

efetiva governança de dados no país, a despeito de mais de um ano de existência da Autoridade Nacional de Proteção de Dados.

Ocorre que não é incomum que situações extremadas de crise deem abertura à paulatina restrição de interesses jurídicos, sob o fundamento da necessidade de contenção de algum problema específico. Nesse ponto, eventos terroristas têm contribuído, por exemplo, para a consolidação de aparatos de vigilância estatal.

O fundamento central da proteção dos dados pessoais, isto é, a autodeterminação informativa e o consentimento, cede espaço à necessidade de contenção da pandemia, tendo em vista que a solicitação de autorização esbarraria em dificuldades operacionais e temporais que inviabilizariam a eficácia das medidas pretendidas.

É necessário pensar em métodos razoáveis de segurança que impeçam acessos não autorizados, coleta, uso, divulgação, cópia, modificação, descarte ou riscos análogos, bem como a necessidade de interrupção do tratamento assim que seja razoável supor que o objetivo para o qual foram coletados não mais subsiste.

A situação se agrava ainda mais quando se constata que a pandemia é contemporânea ao que se chama de infodemia, isto é, uma superabundância de informações que dificulta a localização de fontes e de orientações confiáveis àqueles que necessitam, mormente num contexto digital repleto de *fake news*.

As aplicações tecnológicas atualmente disponíveis têm o potencial de rastrear localizações em tempo real ou metadados que demonstram padrões de comportamento e informações íntimas e que, uma vez admitidas na vida cotidiana, torna-se cada vez mais difícil afastá-las. Dessa forma, ainda que seja admissível a utilização dos dados pessoais, de modo excepcional, temporário e urgente, para a tutela da saúde pública, é fundamental que sejam priorizadas ações de pesquisa, diagnóstico e tratamento efetivos que forneçam ao sistema de saúde infraestrutura

para zelar pelos pacientes e minimizar a ocorrência do vírus, sob pena de nos acomodarmos numa posição de vigilância, obsessão e assédio social que ameaça devassar a privacidade e segregar indivíduos.

As políticas públicas sempre devem buscar um equilíbrio entre as liberdades civis e o interesse coletivo, intentando primar pela proporcionalidade. Se a situação de calamidade traz ameaças que tornam legítima a restrição temporária e excepcional da privacidade, esta deve ser cientificamente justificada e proporcional às necessidades. Nossa saúde e nossa democracia dependem disso.

Neste ponto, é preciso dividir uma inquietação: é possível utilizar dados pessoais temporariamente para gerenciamento de crise sem acarretar, em longo prazo, uma erosão sistemática das garantais fundamentais dos indivíduos? A resposta será construída nos próximos anos, depois que tivermos ultrapassado as graves consequências do período mais intenso da pandemia da COVID-19.

Diante disso, a implementação da Lei Geral de Proteção de Dados Pessoais se mostra imprescindível, haja vista que, densificando o conteúdo do direito fundamental à proteção de dados, consolida e facilita a aplicação pelos setores públicos e privados dos princípios e diretrizes internacionais atinentes a esse direito, os quais são essenciais para permitir que o tratamento de dados pessoais no enfrentamento à pandemia ocorra em equilíbrio com as liberdades fundamentais dos indivíduos.

Nessa senda, quando se analisa o art. 4º da LGPD, que afasta sua aplicação ao tratamento de dados pessoais realizados para fins exclusivos de segurança pública, defesa nacional ou atividades de investigação e repressão de infrações penais (ver inciso III), hipóteses que podem, por analogia, ser interpretadas para o contexto da pandemia, há de se destacar que as medidas adotadas nessas situações devem ser proporcionais e estritamente necessárias ao atendimento do interesse público,

observados o devido processo legal, os princípios gerais de proteção e os direitos do titular, consoante preconiza o § 1º do referido artigo. Não fosse o suficiente, o § 2º do art. 4º da LGPD veda o tratamento de tais dados por pessoa de direito privado, salvo se ocorrer sob a tutela de pessoa jurídica de direito público, assegurado o acompanhamento da Autoridade Nacional de Proteção de Dados.

Por falar em ANPD, ficou demonstrada a importância que a atuação dessa autoridade teria nessa crise, assegurando que a utilização das informações pessoais no combate à pandemia ocorra em observância aos princípios de proteção aos dados pessoais e em respeito aos direitos dos titulares, bem como orientando os agentes de tratamento e editando regulamentos sobre medidas de segurança que devem ser adotadas pelos entes que tiverem acesso aos dados coletados.

Dessa forma, a pandemia deixou evidente a necessidade de um marco regulatório para o direito à proteção de dados pessoais. O Brasil já conta com esse marco e a ANPD, apesar de criada, ainda não conta com qualquer estrutura para que possa funcionar e desempenhar suas funções, as quais são essenciais para a efetividade da referida lei. Necessário, pois, que a Autoridade Nacional passe a funcionar, exercendo suas competências com independência e garantindo efetividade à Lei 13.709/2018.

REFERÊNCIAS

ALEXY, Robert. Colisão de Direitos Fundamentais e Realização de Direitos Fundamentais no Estado de Direito Democrático. *In: Revista de Direito Administrativo,* Rio de Janeiro, v. 217, p. 9, 1999. Disponível em: http://bibliotecadigital.fgv.br/ojs/index.php/rda/article/view/47414.

Acesso em: 11 jun. 2019.

ALVES, Rafael. Tudo sobre o coronavírus – Covid-19: da origem à chegada ao Brasil. – perguntas e respostas sobre o vírus descoberto em dezembro na China e que se tornou emergência de saúde pública de interesse internacional. *Estado de Minas,* 27 fev. 2020. Disponível em: https://www.em.com.br/app/noticia/nacional/2020/02/27/interna_nacional,1124795/tudo-sobre-o-coronavirus-covid-19-da-origem-a-chegada-ao-brasil.shtml. Acesso em: 6 abr. 2020.

AMAZONAS. Governo do Estado. *Wilson Lima anuncia monitoramento remoto de pessoas que chegam pelo aeroporto e aquisição de testes rápidos.* 25 mar. 2020. Disponível em: http://www.amazonas.am.gov.br/2020/03/wilson-lima-anuncia-monitoramento-remoto-de-pessoas-que-chegam-pelo-aeroporto-e-aquisicao-de-testes-rapidos/. Acesso em: 6 abr. 2020.

BBC NEWS. *Coronavirus privacy:* Are South Korea's alerts too revealing? 5 mar. 2020. Disponível em: https://www.bbc.com/news/world-asia-51733145. Acesso em: 6 abr. 2020.

BIONI, Bruno Ricardo. *Proteção de Dados Pessoais:* a função e os limites do consentimento. Rio de Janeiro: Forense, 2019.

BINENBOJM, Gustavo. Da supremacia do interesse público ao dever de proporcionalidade: um novo paradigma para o Direito Administrativo. *Revista de Direito Administrativo.* Rio de Janeiro, jan./mar, 2005.

BRANDEIS, Louis D.; WARREN, Samuel D. The right to privacy. *Harvard Law Review*, v. 4, n. 5, dec. 15, 1890.

BRASIL. Ministério da Saúde. *Painel Coronavírus 2019 (COVID-19) Brasil*. Atualizado em: 20 out. 2020a. Disponível em: https://covid.saude.gov.br/. Acesso em: 20 out. 2020.

BRASIL. SUPREMO TRIBUNAL FEDERAL. *Supremo começa a julgar compartilhamento de dados de usuários de telefonia com o IBGE.* 6 maio 2020b. Disponível em: http://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=442823&ori=1. Acesso em: 17 maio 2020.

CORÉIA DO SUL. *Personal Information Protection Act.* 29 mar. 2011. Disponível em: https://www.privacy.go.kr/cmm/fms/FileDown.do?atchFileId=FILE_000000000830758&fileSn=1&nttId=8186&toolVer=&toolCntKey_1=. Acesso em: 6 abr. 2020.

DAILY MAIL. *South Korea tracks coronavirus patients locations using phone data and CCTV footage- then publishes it online.* Disponível em: https://www.dailymail.co.uk/news/article-8011197/South-Korea-tracks-coronavirus-patients-locations-using-phone-data-publishes-online.html. Acesso em: 22 mar. 2020.

DATA GUIDANCE. *Israel: Government approves mobile tracking to monitor Coronavirus quarantine enforcement.* Disponível em: https://platform.dataguidance.com/news/israel-government-approves-mobile-tracking-monitor-coronavirus-quarantine-enforcement. Acesso em: 22 mar. 2020.

ECDC. European Centre for Disease Prevention and Control. *COVID-19 situation update worldwide, as of 20 October 2020*. 20 out. 2020. Disponível em: https://www.ecdc.europa.eu/en/geographical-distribution-2019-ncov-cases. Acesso em: 20 out. 2020.

EL PAÍS. *Coronavírus de hoje e o mundo de amanhã segundo o filósofo Byung-Chul Han.*. Disponível em https://brasil.elpais.com/ideas/2020-03-22/o-coronavirus-de-hojeeo-mundo-de-amanha-segundoofilosofo-byung-chul-han.html?rel=mas. Acesso em: 24 mar 2020.

G1 PE. *Recife rastreia 700 mil celulares para monitorar isolamento social e direcionar ações contra coronavírus.* 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: 6 abr. 2020.

G1 SE. *Mulher diagnosticada com coronavírus em Sergipe fala sobre preconceito:* 'Isso me deixou mais doente que a própria dor'. 19 mar. 2020. Disponível em https://g1.globo.com/se/sergipe/noticia/2020/03/19/mulher-diagnosticada-com-coronavirus-em-sergipe-fala-sobre-preconceito-isso-me-deixou-mais-doente-do-que-a-propria-dor.ghtml. Acesso em: 6 abr. 2020.

GLOBAL NEWS. "*Yes, this drone is speaking to you": How China is reportedly enforcing coronavirus rules.* Disponível em: https://globalnews.ca/news/6535353/china-coronavirus-drones-quarantine/. Acesso em: 22 mar. 2020.

https://www.gob.pe/institucion/autoridad-nacional-de-proteccion-de-datos-personales/noticias/112036-la-autoridad-nacional-de-proteccion-de-datos-personales-exhorta-a-los-medios-de-comunicacion-a-no-revelar-los-nombres-de-pacientes-de-covid-19-sin-su-consentimiento Acesso em: 2 jun. 2020.

ITS Rio 2016. *Big Data in the Global South Project Report on the Brazilian Case Studies.* Disponível em: https://its-rio.org/wp-content/uploads/2017/01/Big-Data-in-the-Global-South-Project.pdf. Acesso em: 3 nov. 2019.

KIM, Nemo. 'More scary than coronavirus': South Korea's health alerts expose private lives. *The Guardian.* 06 mar. 2020. Disponível em: https://www.theguardian.com/world/2020/mar/06/more-scary-than-coronavirus-south-koreas-health-alerts-expose-private-lives.

Acesso em: 6 abr. 2020.

LINHARES, Marcel Queiroz. O Método da Ponderação de Interesses e a Resolução de Conflitos entre Direitos Fundamentais. *In*: *Revista da Faculdade de Direito da UFPR*, v. 35, p. 232-233, 2001. Disponível em: https://revistas.ufpr.br/direito/article/view/1819. Acesso em: 11 jun. 2019.

MAGRANI, Eduardo. *Entre dados e robôs: ética e privacidade na era da hiperconectividade.* 2. ed. Porto Alegre: Arquipélago Editorial, 2019.

MENDES, Laura Schertel. *Privacidade, proteção de dados e defesa do consumidor – linhas gerais de um novo direito fundamental*. São Paulo: Saraiva, 2014.

MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS DE PERU. *Guía para establecimientos de salud.* Disponível em: https://cdn.www.gob.pe/uploads/document/file/581291/Cartilla-Coronavirus.pdf. Acesso em: 2 jun. 2020.

MOREIRA, Ardilhes; PINHEIRO, Lara. OMS declara pandemia de coronavírus. *G1 – Bem Estar*, 11 mar. 2020. Disponível em: https://g1.globo.com/bemestar/coronavirus/noticia/2020/03/11/oms-declara-pandemia-de-coronavirus.ghtml. Acesso em: 6 abr. 2020.

MOREIRA, Thiago Mattos. As lições da Coréia do Sul no Combate ao Coronavírus. *Época – mundo*, 20 mar. 2020. Disponível em: https://epoca.globo.com/mundo/as-licoes-da-coreia-do-sul-no-combate-ao-coronavirus-1-24315715. Acesso em: 6 abr. 2020.

PEIXOTO, Erick L. C; EHRHARDT JÚNIOR, Marcos. Breves Notas sobre a Ressignificação da Privacidade. *In: Revista Brasileira de Direito Civil*, Belo Horizonte, v. 16, jan./jun. 2018. Disponível em: https://rbdcivil.ibdcivil.org.br/rbdc/article/view/230. Acesso em: 12 jun. 2019.

PERU. *Autoridad Nacional de Protección de Datos Personales supervisará la utilización de los datos de geolocalización em casos infectados y sospechosos de contagio de coronavirus.* Disponível em: https://www.gob.pe/institucion/autoridad-nacional-de-proteccion-de-datos-personales/noticias/127366-autoridad-nacional-de-proteccion-de-datos-personales-supervisara-la-utilizacion-de-los-datos-de-geolocalizacion-en-casos-de-infectados-y-sospechosos-de-contagio-de-coronavirus-covid-19. Acesso em: 02 jun. 2020.

PERU. *La Autoridad Nacional de Protección de Datos Personales exhorta a los medios de comunicación a no revelar los nombres de pacientes de COVID-19 sin su consentimiento.* Disponível em: https://www.gob.pe/autoridad-nacional-de-proteccion-de-datos-personales. Acesso em: 2 jun. 2020.

RAAB, Charles; SZEKELY, Ivan. Data Protection Authorities and Informations Technology. *Computer Law & Security Review*, v. 33, n. 4, ago. 2017. Disponível em: https://www.sciencedirect.com/science/ article/abs/pii/S0267364917301619. Acesso em: 20 abr. 2020

REUTERS. *Coronavirus brings China's surveillance state out the shadows.* Disponível em: https://www.reuters.com/article/us-china-health-surveillance/coronavirus-brings-chinas-surveillance-state-out-of-the-shadows-idUSKBN2011HO. Acesso em: 22 mar. 2020.

RODOTÀ, Stefano. *A vida na sociedade de vigilância* – a privacidade hoje. Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

SCHREIBER, Anderson. *Direitos da Personalidade.* 3. ed. São Paulo: Atlas, 2014.

SOUTH CHINA MORNING POST. *Coronavirus: AI firms deploy fever detection systems in Beijing to fight outbreak.*

Disponível em: https://www.scmp.com/tech/policy/article/3049215/ai-firms-deploy-fever-detection-systems-beijing-help-fight-coronavirus. Acesso em: 22 mar. 2020.

THE NEW YORK TIMES. *In Coronavirus Fight, China Gives Citizens a Color Code, With Red Flags.* Disponível em: https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html. Acesso em: 22 mar. 2020.

THE TELEGRAPH. *Taiwan uses smartphones monitor patients quarantined over virus scare.* Disponível em: https://www.telegraph.co.uk/news/2020/02/03/taiwan-uses-smartphones-monitor-patients-quarantined-virus-scare/. Acesso em: 22 mar. 2020.

VASCONCELOS, Beto; PAULA, Felipe de. A autoridade nacional de proteção de dados: origem, avanços e pontos críticos. *In:* TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. (Coords.). *Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro.* São Paulo: Thomson Reuters Brasil, 2019.

WIRED. *An AI Epidemiologist Sent the First Warnings of the Wuhan Virus.* Disponível em: https://www.wired.com/story/ai-epidemiologist-wuhan-public-health-warnings/. Acesso em: 22 mar. 2020.

WIRED. *How AI is trackin coronavirus outbreak.* Disponível em: https://www.wired.com/story/how-ai-tracking-coronavirus-outbreak/. Acesso em: 22 mar. 2020.

YONHAP NEWS AGENCY. *S. Korea sets guidelines limiting release of private info of coronavirus patients.* Disponível em: https://en.yna.co.kr/view/AEN20200314002000315. Acesso em: 03 out. 2020.