

CRITÉRIOS E LIMITES PARA O TRATAMENTO DE DADOS REALIZADO NO ENFRENTAMENTO DA COVID-19

CRITERIA AND LIMITS FOR DATA PROCESSING PERFORMED IN COVID-19

Graziely Rodrigues Guimarães¹

<https://orcid.org/0000-0002-9953-7902>

Data de Submissão: 05/04/2021

Data de Aceite: 07/06/2021

Resumo: O surgimento de um vírus de alta taxa de transmissão gerou a necessidade da imposição do distanciamento social massivo em todo o mundo. A pandemia da COVID-19 desencadeou – ou reforçou, para alguns países – o uso da tecnologia como meio de monitoramento da população. Pela urgência da situação, as normas tendem a ser flexibilizadas e as decisões governamentais são, muitas vezes, tomadas sem as devidas reflexões acerca do impacto na vida em sociedade. O tratamento de dados deve obedecer a uma série de regras para que se garanta a tutela dos direitos à privacidade, à liberdade e à proteção dos dados pessoais. No entanto, o que se observa é a violação dos direitos dos cidadãos sob a justificativa de uma necessária escolha entre o direito à saúde ou o direito à proteção de dados pessoais. Nesse cenário, o presente artigo visa analisar os critérios e limites para o tratamento de dados pessoais no enfrentamento da COVID-19.

Palavras-chave: Distanciamento Social. Monitoramento. Proteção de Dados. Critérios e Limites.

1 Graduada em Direito pela Universidade de Brasília – UnB.

Abstract: The outbreak of a virus with a high transmission rate has generated the need for the imposition of massive social estrangement all over the world. The COVID-19 pandemic unleashed - or reinforced, for some countries - the use of technology as a means of population monitoring. Due to the urgency of the situation, norms tend to be flexible and government decisions are often taken without due consideration of the impact on life in society. Data processing must comply with a series of rules in order to guarantee the protection of the rights to privacy, freedom and protection of personal data. However, what is observed is the violation of citizens' rights under the justification of a necessary choice between the right to health or the right to personal data protection. In this scenario, the present article aims to analyze the standards and limits for the treatment of personal data collected to confront COVID-19.

Keywords: Social Distancing. Surveillance. Data Protection. Standards and Limits.

1. INTRODUÇÃO

A Organização Mundial da Saúde (OMS) declarou a pandemia do novo coronavírus (SARS-COV-2) em março de 2020, em razão da contaminação de mais de 118 mil pessoas em 114 países, além da morte de mais de 4 mil desses contaminados². Devido à alta taxa de transmissão do vírus³, diversos países receberam recomendações de cientistas e das autoridades de saúde para que adotassem medidas de contenção, tal como a imposição do uso de máscaras em locais públicos e do distanciamento social.

Considerando a dificuldade de realizar o diagnóstico de infecção na população em geral⁴ e que a maioria das pessoas é assintomática ou possui sintomas leves⁵, diversas iniciativas científicas foram e estão sendo desenvolvidas para que, através da coleta de dados pessoais e de geolocalização, se torne possível o rastreamento do vírus. O tratamento das informações coletadas pode se mostrar bastante útil para a elaboração de políticas públicas de combate à COVID-19, já que se pode veri-

2 Hoje (dezembro de 2020), já são mais de 67 milhões de casos e 1,54 milhão de mortes, segundo informações presentes no Painel COVID-19 do Centro de Ciência e Engenharia de Sistemas da Universidade Johns Hopkins (JHU, 2020).

3 O número reprodutivo do SARS-COV-2, ou seja, a quantidade média de pessoas que um sujeito contaminado pode transmitir o vírus, é entre 2,2 e 3,3, o que o classifica como um vírus de alta propagação (ROSSI, 2020).

4 “O diagnóstico da COVID-19 é um desafio em todo mundo. Entre os aspectos que dificultam: 1) o material biológico a ser utilizado, como por exemplo, swab de naso e/ou orofaringe, plasma, soro ou sangue total; 2) a definição do marcador biológico com maiores chances de ser detectado; 3) o tipo de metodologia empregada (métodos virológicos, biologia molecular e imunoenaios); 4) o momento ideal da infecção para a coleta da amostra e tipo ideal de amostra; e 5) a acurácia dos testes de diagnóstico disponíveis. Além disso, com o estado de pandemia declarado pela OMS, há dificuldade de obtenção de insumos para maior disponibilização do teste molecular de detecção do RNA viral, uma vez que este se tornou uma necessidade global.” (MAGNO et al, 2020)

5 PINHEIRO, C. Casos sem sintomas, leves e graves: as diferentes evoluções do coronavírus. **Veja Saúde**, 21/08/2020. Disponível em: < <https://saude.abril.com.br/medicina/casos-sem-sintomas-evolucoes-coronavirus/> >

ficar os contatos feitos pelo infectado⁶ e se as pessoas estão cumprindo o regime de quarentena⁷, por exemplo.

Os países tem pressa na tomada de decisões de enfrentamento à pandemia, uma vez que a doença tem gerado um grande impacto financeiro⁸, seja pela paralisação total ou parcial de diversos setores da economia seja pela distribuição de renda assistencial aos menos favorecidos ou ainda com o alto custo do tratamento dos infectados sintomáticos graves. Como consequência, tem-se a implementação de tecnologias ainda imaturas que, sem as devidas reflexões acerca do impacto na vida em sociedade, podem gerar graves violações ao direito à proteção de dados pessoais das populações (FARIAS, 2020).

Cria-se um aparente dilema entre o direito à proteção de dados pessoais e o direito à saúde. Isso porque, de um lado, busca-se o combate ao coronavírus através de todos os meios disponíveis e, por outro, existem direitos fundamentais que devem ser respeitados mesmo em situações de emergência. Esse conflito é aparente na medida em que inexistente direito fundamental ilimitado. No entanto, apesar de poderem sofrer restrições, não se pode aplicar uma perspectiva de exclusão.

Segundo Roberto Alexy (2015), na hipótese de conflito entre direitos fundamentais, deve-se aplicar a técnica de ponderação. Isso significa que é possível a coexistência de ambos os direitos, sem que haja a necessidade de se declarar a invalidade de um ou de outro. Para tanto, far-se-á a análise das circunstâncias fáticas do caso e, com base no princípio da proporcionalidade, será verificado se o ato que gerou o conflito (*i*) é adequado para o objetivo proposto e (*ii*) é o menos danoso para a concreti-

6 OLIVEIRA, P. Aplicativo ajudará a rastrear contatos de infectados com covid-19. **Agência Brasil**, Brasília, 31/07/2020. Saúde. Disponível em: <<https://agenciabrasil.ebc.com.br/saude/noticia/2020-07/aplicativo-ajudara-rastrear-contatos-de-infectados-com-covid-19>>

7 Governo de MS usa localizadores de celular para monitorar cumprimento da quarentena do coronavírus. **G1 Mato Grosso do Sul**, Cuiabá, 04/04/2020. Disponível em <<https://g1.globo.com/ms/mato-grosso-do-sul/noticia/2020/04/04/governo-de-ms-usa-localizadores-de-celular-para-monitorar-cumprimento-da-quarentena-do-coronavirus.ghtml>>

8 “A natureza da pandemia gerada devido ao COVID-19, provocando a queda abrupta da atividade econômica em praticamente todos os países, gerou uma desvalorização significativa em todas as bolsas mundiais” (SAMPAIO, 2020)

zação do fim almejado. Por fim, analisa-se a necessidade de cerceamento de um direito em prol da concretização de outro.

Finalizados estes passos, é possível chegar a conclusão de qual direito deve prevalecer. Diante disso, o tratamento de dados pessoais coletados para fins de enfrentamento à COVID-19 deve ser feito de maneira adequada e não excessiva ao fim almejado. Nesse sentido, o presente artigo visa analisar os limites e os critérios que devem ser levados em consideração quando do tratamento dos dados coletados para combate à propagação do novo coronavírus.

2. CONTEXTO MUNDIAL

Nem todos os países do mundo possuem uma legislação específica para a proteção de dados pessoais de seus cidadãos e alguns sequer reconhecem esse direito diretamente⁹. A partir desse cenário, concomitante à pandemia do novo coronavírus e à necessidade de rastreamento da população para verificar possíveis infectados ou para analisar o cumprimento das medidas de distanciamento social, nota-se uma grande pluralidade no tratamento de dados pessoais coletados pelos diversos aplicativos e dispositivos elaborados com o objetivo de facilitar o combate ao vírus.

Nesse contexto, surgem questionamentos acerca dos desafios éticos, legais e técnicos que permeiam a coleta, o acesso, o compartilhamento e uso dos dados pessoais em vários países do mundo.

2.1. Índia

A Índia ainda não possui uma legislação específica para a proteção de dados pessoais, logo a proteção é feita indiretamente em atenção ao direito à liberdade¹⁰. Apesar da ausência legislativa, a Suprema Corte

⁹ Segundo dados da UNCTAD (2020), apenas 66% dos países possuem legislação específica para a proteção de dados pessoais. O restante não possui legislação específica ou encontram-se na fase da tramitação de projeto de lei ou não há informações disponíveis.

¹⁰ O art. 21 da Constituição Indiana de 1949 prevê “Nenhuma pessoa será privada da vida ou da liberdade pessoal, exceto se estabelecido em lei” (tradução livre).

Indiana decidiu, em 2017, no caso *Puttaswamy vs. Índia*, que a privacidade seria um direito fundamental protegido pela sua Constituição e, em 2018, o Tribunal requereu que o Governo elaborasse regras rígidas acerca da proteção de dados pessoais. (BURMAN; RAI, 2020). Diante disso, em 2019, foi criado um projeto de lei para tratar sobre o assunto. No entanto a previsão é que seja aprovado pelo Parlamento somente em 2021.

Conforme supracitado, o vácuo normativo torna o direito suscetível a violações, o que se pode verificar na iniciativa do governo indiano de fabricar braceletes de monitoramento que coletam dados de geolocalização em tempo real, além de sinais vitais do usuário, como batimentos cardíacos, temperatura e nível de oxigenação (GHOSAL, 2020). Ademais, este dispositivo, utilizado juntamente a um aplicativo, permite que as autoridades apliquem medidas restritivas de liberdade, já que o *software* traça um perímetro virtual de circulação permitida para o usuário infectado. Caso haja qualquer desrespeito, as autoridades estão autorizadas a intervir.

A coleta de dados é abrangente e desproporcional ao fim almejado¹¹ e, portanto, viola o direito à privacidade, previsto tanto na Constituição Indiana quanto em diversos diplomas internacionais do qual o país é signatário¹².

2.2. Coreia do Sul

Após a epidemia do MERS em 2015, também causada por um coronavírus, a Coreia do Sul aprovou a *Personal Information Protection Act*, le-

11 “Em um documento técnico da entidade, afirmam que é possível a identificação de comportamentos considerados suspeitos, checar o que o usuário faz em determinados dias da semana, em quais estabelecimentos consome comida, quais são seus contatos mais frequentes, assim como contatos ocasionais como motoristas de aplicativo, sabem com quem a pessoa esteve e por quanto tempo, entre outras informações.” (FARIAS, 2020)

12 A Declaração Universal de Direitos Humanos, por exemplo, foi assinada pelo Índia e prevê em seu art. 12 que “Ninguém será sujeito à interferência na sua vida privada, na sua família, no seu lar ou na sua correspondência, nem a ataque à sua honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques” (ONU, 1948).

gislação que excepcionou, nos casos de urgência de saúde, segurança ou bem-estar, a não incidência das “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” (MODESTO; EHRHARDT, 2020, p. 149). Dessa forma, criou-se um cenário propício a coleta de dados pessoais de forma massiva durante o enfrentamento do SARS-COV-2. Apesar de a divulgação dos dados ser de forma anonimizada, tornou-se possível, por agregação, a identificação do titular, uma vez que se trata de uma quantidade considerável de dados¹³.

Para exemplificar, tem-se o caso de um coreano que contraiu o coronavírus em decorrência de contato com um instrutor de uma palestra. Após o diagnóstico, o Governo enviou mensagens a toda a população, nas quais constavam diversos dados do infectado, como idade, sexo, local de residência e de trabalho, ocasião em que contraiu, locais por ele visitado após a infecção, dentre outros¹⁴.

É importante salientar que a Coreia do Sul se tornou um dos países com os melhores resultados no combate ao novo coronavírus. Foram adotadas diversas medidas para alcançar esse resultado, tal como a testagem em massa e o incentivo ao *home office*. Diante desse cenário, surge uma reflexão acerca da coleta e da divulgação dos dados coletados, já que, com tantas medidas de prevenção e de combate à propagação do vírus, o tratamento dos dados aparenta ser desproporcional e excessivo.

2.3. Brasil

Com o objetivo de viabilizar a realização das entrevistas oficiais feitas pelo IBGE de forma não presencial, foi editada a Medida Provisó-

13 A anonimização dos dados não é completa; e pesquisas indicam a reversão do processo através da agregação de 15 dados do titular.

14 “Toda essa riqueza de informações que o governo divulga em seus alertas é fruto da 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”. (MODESTO & EHRHARDT, 2020)

ria n. 954, de abril de 2020, que buscou a coleta de dados dos cidadãos brasileiros através do compartilhamento compulsório das informações constantes nas bases de dados das empresas de telecomunicações com o Instituto Brasileiro de Geografia e Estatística (IBGE). A partir das informações coletadas nas entrevistas, seria gerado conhecimento essencial para a elaboração de políticas governamentais para enfrentar o novo coronavírus.

Após sua edição, a MP n. 954/2020 foi alvo de diversas críticas em razão de aparente violação a direitos fundamentais constitucionalmente tutelados. Isso porque o objetivo proposto pela medida era genérico e insuficiente para justificar o compartilhamento e tratamento de dados. Ademais, uma vez que se tratava de uma finalidade ampla, não era possível analisar se aquele meio era realmente o mais adequado para o fim almejado. Outro ponto da MP n° 954/2020 que foi criticado foi quanto à ausência de transparência de como os dados serão utilizados e publicizados.

Em razão do caráter de urgência, a medida provisória careceu de detalhamentos essenciais que demonstrassem sua necessidade para o fim almejado e as lacunas geraram brechas para a violação de direitos fundamentais, tais como a dignidade da pessoa humana, a inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas e o sigilo dos dados e a autodeterminação informativa, previsto nos art. 1º, inciso III, e art. 5º, incisos X e XII, da Constituição Federal.

Diante disso foram propostas diversas ações diretas de constitucionalidade (ADIs). A principal delas foi a ADI n. 6387, proposta pelo Conselho Federal da Ordem dos Advogados do Brasil, com pedido de medida cautelar de urgência. A Relatora, Ministra Rosa Weber, entendeu que, ao prever o compartilhamento de nomes, números telefônicos e endereços, a MP n. 954/2020 estaria realizando tratamento de dados pessoais e, portanto, estaria sujeita a observar os direitos à liberdade, à privacidade e à personalidade.

Assim, inexistindo (i) justificativa consistente e legítima para a coleta de dados¹⁵, além de (ii) condições para a avaliação da adequação e

15 “[...] o único dispositivo da MP n. 954/2020 a dispor sobre a finalidade e o modo de utilização dos dados objeto da norma é o § 1º do seu art. 2º. E esse limita-se a enunciar que os dados em questão serão utilizados exclusivamente pela Fundação IBGE para a

necessidade dos dados coletados, a MP n. 954/2020 estaria violando os limites delineados pela proteção constitucional. Ademais, a Relatora entendeu que restavam ausentes as garantias de segurança e de anonimização para o tratamento dos dados compartilhados, o que motivou a suspensão da eficácia da medida provisória.

Outro caso importante para entender a utilização da tecnologia como auxiliar para o combate ao novo coronavírus é o Sistema de Monitoramento Inteligente (Simi), lançado em São Paulo com o objetivo de utilizar os dados georreferenciais dos celulares para identificação de aglomerações e monitoramento do grau de isolamento. Os dados também seriam utilizados para a promoção de ações de advertência e de orientação à população.

Esse sistema também foi contestado judicialmente, no entanto o entendimento adotado pelo Tribunal de Justiça de São Paulo divergiu da decisão tomada pelo Supremo Tribunal Federal no julgamento da ADI n. 6387. Isso porque os dados coletados pelo Governo de São Paulo eram anonimizados, estatísticos e agregados e havia um claro interesse público no combate ao coronavírus. Dessa forma, os princípios constitucionais de liberdade, privacidade e personalidades estariam garantidos.

Importante também analisar o caso de uma mulher moradora do Sergipe que após uma viagem com conexão em São Paulo contraiu o vírus. Antes mesmo de confirmado o diagnóstico, ela teve seus dados vazados, gerando uma série de ataques virtuais¹⁶. Os dados referentes à saúde do titular são sensíveis e quando tratados devem ser adotadas medidas de segurança para garantir que não haja qualquer tipo de vazamento ou para que, no caso de exposição, haja o menor dano possível, o que não foi observado no caso.

produção estatística oficial, com o objetivo de realizar entrevistas em caráter não presencial no âmbito de pesquisas domiciliares. Não delimita o objeto da estatística a ser produzida, nem a finalidade específica, tampouco a amplitude. Igualmente não esclarece a necessidade de disponibilização dos dados nem como serão efetivamente utilizados” (STF, 2020).

16 Mulher diagnosticada com coronavírus em Sergipe fala sobre preconceito: ‘Isso me deixou mais doente do que a própria dor’. *G1 Sergipe*, 19.03.2020. 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>>

Outro evento que representa clara violação ao direito à proteção de dados pessoais ocorreu após o governo estadual do Amazonas ter determinado a quarentena a todos os passageiros que desembarcassem no Aeroporto Internacional Eduardo Gomes e ainda que estes instalassem um aplicativo em seus celulares para que o fosse feito um monitoramento de suas localizações, em tempo real, por 14 dias.

Por fim, vale ressaltar que a Lei n. 13.979, de 06 de fevereiro de 2020, que tratou sobre medidas de emergência para o enfrentamento da COVID-19, representou também uma flexibilização no tratamento de dados. Isso porque prevê em seu art. 6º o compartilhamento obrigatório de dados que facilitem a contenção da propagação do novo coronavírus¹⁷ (BARROS, 2020).

3. O PERIGO DA VIGILÂNCIA CONTÍNUA

Alguns países que se destacaram na contenção da propagação da COVID-19 obtiveram esse sucesso em razão de uma vasta infraestrutura consolidada em todo o território de “câmeras, algoritmos de reconhecimento facial e uma grande integração das bases de dados do governo” (BARILI, 2020), o que permitiu o fácil rastreamento dos indivíduos. No Brasil, apesar de existente¹⁸, essa não era uma infraestrutura bastante desenvolvida, motivo pelo qual buscou-se o aperfeiçoamento das tecnologias de captação de dados.

17 “Art. 6º É obrigatório o compartilhamento entre órgãos e entidades da administração pública federal, estadual, distrital e municipal de dados essenciais à identificação de pessoas infectadas ou com suspeita de infecção pelo coronavírus, com a finalidade exclusiva de evitar a sua propagação.

§ 1º 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.

§ 2º 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.” (BRASIL, 2020)

18 “Na ocasião da Copa do Mundo Fifa (Federação Internacional de Futebol) de 2014 foram implementados 14 CICC’s (Centros Integrados de Comando e Controle) para monitoria dos espaços públicos, sendo 2 de administração nacional e 12 de administração regional (Ministério do Esporte, 2014)” (BATISTA; FARINIUK; MELLO, 2016)

Foram desenvolvidos aplicativos do governo para rastreamento de infectados e para alertas de riscos de infecção¹⁹, além de aplicativos com o objetivo de distribuir renda para os mais desfavorecidos²⁰. Essas ferramentas geram uma coleta massiva de dados da população, seja de forma voluntária ou involuntária, além de permitirem a inserção de uma política de controle e vigilância ativa pelo Estado (BARILI, 2020).

Conforme supracitado, a pressão para conter o problema pode gerar uma flexibilização legislativa. No Brasil, a Lei n. 13.979/2020 previu o compartilhamento obrigatório de dados pessoais essenciais para o combate ao novo coronavírus, revogando, durante seu período de vigência, qualquer restrição imposta pela Lei Geral de Proteção de Dados Pessoais (Lei n. 13.709/2018).

Surgem alguns riscos a partir dessa naturalização do monitoramento em tempos de emergências. Primeiramente, é importante ressaltar o Estado já se mostrou diversas vezes incapaz de realizar uma proteção eficiente dos dados pessoais da população, o que pode ser depreendido dos recentíssimos casos de vazamento de dados de brasileiros usuários do Sistema Único de Saúde²¹ e dos ataques hackers feitos em diversos tribunais e ministérios²².

Ademais, existe um grande risco de que a política de vigilância à população se torne permanente, uma vez que as estruturas tecnológicas aperfeiçoadas não serão descartadas, muito menos os dados coletados. Estes podem ser disponibilizados para outros fins, em razão da facilidade de se criar um novo motivo para a continuidade do monitoramento,

19 Os aplicativos Coronavírus SUS e guardiões da Saúde foram duas das inovações que buscavam o rastreio de infectados. (OLIVEIRA, 2020 e GALVÃO, 2020)

20 O aplicativo da Caixa – Auxílio Emergencial foi desenvolvido com o intuito de fornecer proteção emergencial a um grupo de pessoas mais desfavorecidas durante o período de crise sanitária e de saúde pública causada pela COVID-19. Disponível em: <<https://www.caixa.gov.br/auxilio/Paginas/default2.aspx> >

21 BERTONI, E. **O novo vazamento de dados na Saúde e suas consequências.** Nexo Jornal, 02/12/2020. Disponível em <<https://www.nexojornal.com.br/expres-so/2020/12/02/O-novo-vazamento-de-dados-na-Sa%C3%BAde.-E-suas-consequ%C3%AAs>>

22 DA COSTA, M. **Brasil sofre seu maior ataque hacker da história.** *Veja*, 05/11/2020. Disponível em: <<https://veja.abril.com.br/blog/radar-economico/brasil-sofre-seu-maior-ataque-hacker-da-historia/>>

já que “sempre há uma nova emergência no horizonte” (HARARI *apud* BARILI, 2020). Essa permanente vigilância é um risco contra a democracia, pois o tratamento de dados massivos da população já se mostrou um meio de manipulação e controle das pessoas, através da influência do Governo na tomada de decisão dos cidadãos.

Daí advém a necessidade de leis que assegurem os direitos fundamentais, além de uma autoridade independente que monitore e reporte os abusos no tratamento de dados de maneira objetiva. No Brasil, a Autoridade Nacional de Proteção de Dados (ANPD) está ligada diretamente ao Poder Executivo, o que gerou grandes críticas dos diversos estudiosos da área. Dentre os principais motivos, ressalta-se a inadequação frente às legislações internacionais, o que pode representar um óbice para o compartilhamento internacional de dados, e se questiona se essa subordinação não deslegitimaria a instituição, já que a atuação da ANPD estaria diretamente sujeita às trocas partidárias e sua capacidade fiscalizatória seria reduzida pela influência do Governo (SIMÃO; OMS; TORRES, 2019).

4. UM PONTO DE EQUILÍBRIO: O USO LEGÍTIMO DE DADOS NO COMBATE À COVID-19

Com base no exposto, faz-se necessário explicitar alguns parâmetros que devem ser observados quando da coleta de dados da população para fins de combate ao novo coronavírus. Encontrado esse ponto de equilíbrio, restarão resguardados os direitos à dignidade, à liberdade e à privacidade, estreitamente ligados à proteção de dados pessoais, e o direito à saúde (BIONI et al, 2020).

Inicialmente, deve ser analisada a necessidade do uso dos dados para a elaboração da política pública de enfrentamento à COVID-19. Para tanto, deve haver uma motivação fundamentada em evidências científicas, além do uso dos dados estar previsto em lei e o compartilhamento ser formalizado através de instrumento contratual. O objetivo é evitar a arbitrariedade, reforçar a legitimidade da medida e permitir uma maior vinculação (BIONI et al, 2020).

Posteriormente, passa-se para a fixação da finalidade do tratamento de dados, ou seja, é necessário delimitar de forma expressa para que

serão utilizados os dados coletados, além de demonstrar que todos os dados coletados são de extrema importância para a finalidade almejada. Através desses procedimentos, será possível reduzir as chances de uso dos dados para fins discriminatórios abusivos (BIONI et al, 2020).

O terceiro passo diz respeito ao tempo de uso daqueles dados. É importante delimitar por quanto tempo o controlador poderá usar os dados disponíveis, além de definir uma forma segura de descarte. Essa limitação pode evitar o uso dos dados para outros fins, uma vez que estes serão conservados somente pelo tempo necessário (BIONI et al, 2020).

Analisa-se, ainda, se estão sendo observados e aplicados todos os meios de proteção e segurança dos dados. Os dados devem ser anonimizados, aplicando-se as melhores técnicas de remoção de identificadores para garantir o maior nível possível proteção ao titular. Ademais, é necessário utilizar mecanismos que evitem incidentes de segurança e amenizem os danos nos casos de vazamento (BIONI et al, 2020).

Por fim, faz-se necessário garantir a publicidade e transparência de todo o tratamento dos dados, evitando o uso de maneira discriminatório ou discricionária (BIONI et al, 2020).

CONSIDERAÇÕES FINAIS

A tecnologia é instrumento facilitador da vida humana e os problemas que surgem a partir disso dizem respeito ao modo como o ser humano a utiliza. Por isso, faz-se necessária a criação de mecanismos de regulação do uso, de modo a proteger os direitos e garantias individuais e coletivos dos indivíduos. Apesar de a pandemia da COVID-19 ter desencadeado um aumento no uso de tecnologias de monitoramento, a legislação veda o uso discricionário e ilimitado. Não há necessidade de exclusão do direito à proteção de dados em prol do direito à saúde. É possível a coexistência de ambos, se a limitação respeitar determinados parâmetros.

O que se observa dos casos analisados é que, inicialmente, a lacuna normativa acerca da proteção de dados na Índia gerou um ambiente propício a mais violações. No entanto, também é possível que o legislador atue de forma abusiva, causando graves violações aos direitos fundamentais, como se depreende da Coreia do Sul. Já no Brasil, apesar de uma

legislação específica vigente, existem casos de abusos, como o aplicativo Coronavírus – SUS, ao não prever um ciclo de vida para os dados coletados, o que pode gerar desvio de finalidade (FANTINI, 2020).

Ademais, quanto à entrada massiva da tecnologia na vida coletiva, é importante se questionar sobre os riscos que a naturalização do monitoramento da população pode gerar no futuro. De um lado, tem-se um Estado que já se demonstrou pouco eficiente na proteção e segurança dos dados pessoais e, de outro, há a manutenção das estruturas tecnológicas, através da atribuição de novas finalidades, justificáveis por um suposto interesse público.

Em um contexto de pré-coleta dos dados, para a elaboração de qualquer medida que exija o tratamento de dados é necessário observar os princípios relativos à motivação, à previsão legal, à existência de instrumento formal, à finalidade, à minimização, ao ciclo de vida, à (pseudo) anonimização, à segurança da informação, à transparência e ao código aberto. Caso a violação já tenha se concretizado ou esteja em curso, é importante lembrar da atuação de uma autoridade de proteção de dados independente como fiscalizadora, interventora e aplicadora de sanções. No Brasil, a ANPD é subordinada ao Poder Executivo, o que pode deslegitimar seus atos no âmbito internacional, criando óbices para o compartilhamento de dados com outros países.

BIBLIOGRAFIA

ALEXY, Robert. **Colisão de direitos fundamentais e realização de direitos fundamentais no Estado de Direito Democrático**. Revista de Direito Administrativo, Rio de Janeiro, v. 217, 2015.

BARILI, F. **Coronavírus: um intensificador do Estado de Vigilância. Os Dados e o Vírus: Pandemia, Proteção de Dados e Democracia**. Data Privacy Brasil Publicações: São Paulo, 2020.

BARROS, R. “Quis Custodiet Ipsos Custodies”: A Naturalização da vigilância em massa em tempos de emergência. **Os Dados e o Vírus: Pandemia, Proteção de Dados e Democracia**. Data Privacy Brasil Publicações: São Paulo, 2020.

BATISTA, M.; FARINIUK, T.; MELLO, S. **Smartsurveillance em Aplicações Recentes no Brasil: Um Estudo de Caso nas Cidades de Recife e Curitiba**. Revista de Gestão e Secretariado - GeSec, São Paulo, v. 7, n. 2, pp. 104-137, mai./ago. 2016.

BERTONI, E. O novo vazamento de dados na Saúde e suas consequências. **Nexo Jornal**, 02/12/2020. Disponível em <<https://www.nexojornal.com.br/expresso/2020/12/02/O-novo-vazamento-de-dados-na-Sa%C3%BAdE.-E-suas-consequ%C3%Aancias>> Acesso em 02/12/2020.

BIONI, B. et al. **Privacidade e Pandemia: recomendações para o uso legítimo de dados no combate à COVID-19**. Data Privacy Brasil, São Paulo, 13 abr. 2020.

BRASIL. Lei nº 13.979, de 6 de Fevereiro de 2020. **Dispõe sobre as medidas para enfrentamento da emergência de saúde pública de importância internacional decorrente do coronavírus responsável pelo surto de 2019**. Disponível em: <<https://www.in.gov.br/en/web/dou/-/lei-n-13.979-de-6-de-fevereiro-de-2020-242078735>> Acesso em 02/12/2020.

BURMAN, A.; RAI, S. What is in India's Sweeping Personal Data Protection Bill? **Carnegie India**. 09 de mar. 2020. Disponível em: < <https://carnegieindia.org/2020/03/09/what-is-in-india-s-sweeping-personal-data-protection-bill-pub-80985#:~:text=What%20is%20the%20personal%20data,respect%20to%20their%20personal%20information.> >. Acesso em: 02/12/2020.

DA COSTA, M. Brasil sofre seu maior ataque hacker da história. **Veja**, 05/11/2020. Disponível em: <https://veja.abril.com.br/blog/radar-economico/brasil-sofre-seu-maior-ataque-hacker-da-historia/> Acesso em 02/12/2020.

FANTINI, L. Coronavírus -SUS: aspectos relevantes da privacidade e proteção de dados e tecnologia de vigilância. **Os Dados e o Vírus: Pandemia, Proteção de Dados e Democracia**. Data Privacy Brasil Publicações: São Paulo, 2020

FARIAS, G. **Vigilância Moviada a Dados como Mecanismo de Combate à COVID_19 e seus Limites Éticos envolvidos na Proteção de Dados Pessoais**. Revista Caderno Virtual. Vol. 2, n. 47, 2020.

GALVÃO, W. Covid-19: aplicativo reformulado com apoio da UnB monitora pacientes. **Correio Brasiliense**, 24/07/2020. Disponível em: <https://www.correiobraziliense.com.br/app/noticia/cidades/2020/07/24/interna_cidadesdf,875127/covid-19-aplicativo-reformulado-com-apoio-da-unb-monitora-pacientes.shtml > Acesso em 02/12/2020.

G1. Governo de MS usa localizadores de celular para monitorar cumprimento da quarentena do coronavírus. **G1 Mato Grosso do Sul**, Cuiabá, 04/04/2020. Disponível em: <<https://g1.globo.com/ms/mato-grosso-do-sul/noticia/2020/04/04/governo-de-ms-usa-localizadores-de-celular-para-monitorar-cumprimento-da-quarentena-do-coronavirus.ghtml>>. Acesso em 02/12/2020.

GHOSAL, A. **India to use wristband to monitor locations, temperatures of COVID-19 patients**. Global News. 22 abr. 2020. Disponível

em: < <https://globalnews.ca/news/6851463/coronavirus-india-wrist-bands/> >. Acesso em 02/12/2020.

JHU. Painel COVID-19 do Centro de Ciência e Engenharia de Sistemas da Universidade Johns Hopkins. Disponível em: <https://www.arcgis.com/apps/opsdashboard/index.html#/bda7594740fd-40299423467b48e9e_cf6> Acesso em 02/12/2020.

MAGNO, L. et al. **Desafios e propostas para ampliação da testagem e diagnóstico para COVID- 19 no Brasil.** Ciência & Saúde Coletiva. Vol. 25, n. 9, Rio de Janeiro: set. 2020. Revista Eletrônica Direito e Sociedade. Canoas, v. 8, n. 2, p. 143-161, ago. 2020.

MODESTO, J.; EHRHARDT, M. **Danos colaterais em tempos de pandemia: preocupações quanto ao uso dos dados pessoais no combate a COVID-19.** Revista Eletrônica Direito e Sociedade. Canoas, v.8, n. 2020.

OLIVEIRA, P. Aplicativo ajudará a rastrear contatos de infectados com covid-19. **Agência Brasil**, Brasília, 31/07/2020. Saúde. Disponível em: <<https://agenciabrasil.ebc.com.br/saude/noticia/2020-07/aplicativo-ajudara-rastrear-contatos-de-infectados-com-covid-19>>

OMS. **World Health Organization Director General's Opening Remarks at The Media Briefing on Covid-19.** Disponível em: <<https://www.who.int/director-general/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-covid-1911-march-2020>> Acesso em 02/12/2020.

PINHEIRO, C. Casos sem sintomas, leves e graves: as diferentes evoluções do coronavírus. **Veja Saúde**, 21/08/2020. Disponível em: <<https://saude.abril.com.br/medicina/casos-sem-sintomas-evolucoes-coronavirus/>> Acesso em 02/12/2020.

PINHEIRO, C. Casos sem sintomas, leves e graves: as diferentes evoluções do coronavírus. **Veja Saúde**, 21/08/2020. Disponível em: <<https://saude.abril.com.br/medicina/casos-sem-sintomas-evolucoes-coronavirus/>> Acesso em 02/12/2020.

ROSSI, A. Contágio Rápido e Silencioso: a Matemática do Coronavírus. **Piauí**. 31 jan. 2020. Disponível em: <<https://piaui.folha.uol.com.br/contagio-rapido-e-silencioso-matematica-do-coronavirus/>>. Acesso em 02/12/2020.

SAMPAIO, J. **Covid-19 e Mercado Financeiro**. Fundação Getúlio Vargas. Escola de Economia de São Paulo Projetos. 2020.

SIMÃO, B.; OMS, J.; TORRES, L. **Autoridades de Proteção de Dados na América Latina: um Estudo dos Modelos Institucionais da Argentina, Colômbia e Uruguai**. Instituto Brasileiro de Defesa do Consumidor, São Paulo, 03 mai. 2019.

STF. **Ação Direta de Inconstitucionalidade n. 6.387**. Relatora Ministra Rosa Weber, julgado em 07/05/2020. Disponível em: <<https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=754357629>> Acesso em 02/12/2020.

UNCTAD. **Data Protection and Privacy Legislation Worldwide**. 02/04/2020. Disponível em: <<https://unctad.org/page/data-protection-and-privacy-legislation-worldwide>>. Acesso em 02/12/2020.