(DES)LIBERDADE VIRAL NA PANDEMIA: UMA RELEITURA DA ESCALADA POR DADOS PESSOAIS E SEUS IMPACTOS À LUZ DOS DIREITOS DA PERSONALIDADE E A PROTEÇÃO DE DADOS

VIRAL (UN)FREEDOM IN PANDEMIA: A REVIEW OF CLIMBING BY PERSONAL DATA AND ITS IMPACTS IN THE LIGHT OF PERSONALITY RIGHTS AND DATA PROTECTION

Oscar Ivan Prux [1]
Kevin Henrique de Sousa Piai [2]

RESUMO: Desde o final de 2019, o mundo luta contra a corona vírus (COVID-19). Em resposta ao que a Organização Mundial da Saúde (OMS) rotulou de pandemia, governos em todo o mundo têm usado tecnologia para conter a propagação do vírus e manter as pessoas seguras. Apesar da pressão do tempo em prol da prevenção de vidas, as medidas de violação de direitos devem ser tratadas com cautela e consideradas extraordinárias. O presente artigo pretende analisar a repercussão da vigilância virtual durante a pandemia, em especial sob o espectro do direito à privacidade e proteção de dados no período da crise e no futuro. O presente estudo se concentrará em três principais categorias que governos de todo mundo têm avançado: i) coleta e uso de dados de saúde, ii) rastreamento e localização geográfica e iii) parcerias público-privadas. Através de estudo empírico em direito comparado, apresentará experiências reais exercidas por governos, empresas de tecnologia e agências internacionais. Trata-se de análise doutrinária com revisão bibliográfica e documental referenciada que, após exemplificação prática, situa o atual estágio de investidas governamentais para acesso a dados sensíveis de sua população, apresentando sugestões para minimização da violação de dados pessoais sensíveis e massivos.

Palavras-chaves: proteção de dados; privacidade; saúde; pandemia; covid-19.

ABSTRACT: Since the end of 2019, the world has been fighting the corona virus (COVID-19). In response to what the World Health Organization (WHO) has labeled a pandemic, governments around the world have been using technology to stem the spread of the virus and keep people safe. Despite the pressure of time, with a view to preventing lives, measures of violation of rights must be treated with caution and considered extraordinary. This article intends to analyze the impact of virtual surveillance, during the pandemic under the spectrum of the right to privacy and data protection during this crisis and in the future. This study will focus on three main categories that governments around the world have advanced: i) collection and use of health data, ii) tracking and geographic location and iii) public-private partnerships. Through an empirical study in comparative law, presenting real experiences exercised by governments, technology companies and international agencies. It is a doctrinal analysis with referenced bibliographic and documentary review that, after practical example, situates the current stage of governmental advances to access sensitive data of its population, presenting sugestion for minimizing the violation of sensitive and massive personal data.

Keywords: data protection; privacy; health; pandemic; covid-19.

1 Pós-doutor pela Faculdade de Direito da Universidade de Lisboa, Portugal (FDUL). Doutor em Direito das Relações Sociais pela Pontifícia Universidade Católica de São Paulo (PUC SP). Mestre em Direito das Relações Sociais pela Universidade Estadual de Londrina. Especialista em Teoria Econômica pela Fundação Faculdade Estadual de Ciências Econômicas de Apucarana. Professor do Programa de Pós-graduação Stricto Sensu em Ciências Jurídicas da Universidade Cesumar (UniCesumar). Mediador judicial.

2 Mestrando em Direitos da Personalidade pela Universidade Cesumar. Bolsista PROSUP/CAPES. Pesquisador do Laboratório de Pesquisa em Direito Privado e Internet da Universidade de Brasilia (LAPIN/UnB). Pesquisador do Observatório de Direito Eletrônico da UniCesumar. Ex-bolsista do Summer Academic Fellowship Program pela Universidade de Harvard.

1. INTRODUÇÃO

A doença infecciosa causada pela corona vírus, síndrome respiratória aguda grave 2 (SARS-CoV-2), tem mobilizado ações econômicas, políticas e sociais jamais vistas anteriormente. Nesse cenário, governos se mobilizam em investidas legislativas específicas para o enfretamento a pandemia, desde propostas de isolamento, quarentena, uso de máscaras, obrigatoriedade do distanciamento social até a interoperabilidade de dados pessoais, inclusive sensíveis, mediante parcerias público-privadas, que se tornaram possíveis através do rastreamento com precisão de sensores de localização integrados à *smartphones*, utilizados na finalidade de monitoramento e contenção da propagação da doença.[3]

O momento crítico vivido por todos países, revela que a grande diferença entre a COVID-19[4] e demais surtos pandêmicos anteriormente vividos, se estabelece na propagação da doença e da informação nos meios digitais concomitantemente, em uma sociedade extremamente conectada.

De toda sorte, a tecnologia pode e deve desempenhar um papel importante durante esse esforço para salvar vidas, referindo-se exemplificativamente, divulgar mensagens de saúde pública e formas de aumentar o acesso aos cuidados de saúde. No entanto, as medidas excepcionais não devem se protrair no tempo, pois os mesmos instrumentos que servem à fins nobres têm potencial para serem desvirtuados acabarem utilizado no controle e manipulação social. Conforme será demonstrado neste trabalho, o aumento nos poderes de vigilância digital do Estado, como, dentre outras situações, a obtenção de acesso a dados de localização de telefones celulares, ameaça a privacidade, a liberdade de expressão e locomoção, sendo que pode violar direitos e diminuir a confiança nas autoridades públicas, prejudicando a eficácia das políticas sanitárias de combate a pandemia e, posteriormente, o bom desenvolvimento social. Tais medidas também representam um risco de discriminação e podem prejudicar desproporcionalmente comunidades já marginalizadas, seja no processo tecnológico, seja em decorrência das condições sociais em que convivem. Não se deve ignorar a advertência contida na obra "Tecnopolíticas da Vigilância – Perspectivas da Margem": "Mesmo que o big data possa ser configurado para outros usos, estes não apagam suas origens em um projeto de extração fundado na indiferença formal em relação às populações que conformam tanto sua fonte de dados quanto seus alvos finais"[5]. Na prática, um instrumento com enorme potencial de utilidade, mas que pode resultar em uso alheio a aspectos legais e desprovido do recomendável conteúdo ético e moral.

Importante referir que estamos passando por tempos incomuns, mas as leis que salvaguardam direitos humanos e privacidade ainda se aplicam.[6] Na verdade, a estrutura dos direitos humanos é projetada para garantir que diferentes direitos possam ser cuidadosamente equilibrados para proteger os indivíduos e as sociedades em geral, independente do momento vivenciado. Estados e organizações mesmo em situações que exigem providências decisivas (como a edição de Medidas Provisórias) nem mesmo sob

3 DIEB, Daniel; GOMES, Helton Simões. Governo vai monitorar celular para controlar aglomeração na pandemia. [S.l.]: UOL, 2 abr. 2020. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2020/04/02/para-combater-a-covid-19-o-governo-federal-vai-monitorar-o-seu-celular.htm. Acesso em: 7 set. 2020.
4 ALLAM, Zaheer; JONES, David S. "On the coronavirus (Covid-19) outbreak and the smart city network: Universal data sharing standards coupled with artificial intelligence (AI) to benefit urban health monitoring and management". *Healthcare* (Basel, Switzerland), v.8, n.1, 2020. Disponível em: https://doi.org/10.3390/healthcare8010046.
5 Tecnopolíticas da vigilância Boitempo Editorial. Edição do Kindle. Posição 264, p.21, 2019.
6 Resolución 01/20. Pandemia y Derechos Humanos en las Américas. Comisión Interamericana de Derechos Humanos. Disponível em: http://oas.org/es/cidh/decisiones/pdf/Resolucion-1-20-es.pdf.

amparo de normas de caráter emergencial, podem ser desconsiderados direitos como a privacidade e a liberdade de expressão, mesmo que em nome do combate a uma crise de saúde pública. O regime de exceção e as novas medidas e normas que surgem não legitimam desconsiderar direitos fundamentais[7].

Pelo contrário, a proteção dos direitos humanos e direitos fundamentais também promove a saúde pública.[8] Agora, mais do que nunca, governos devem garantir rigorosamente que quaisquer restrições a esses direitos estejam de acordo com as salvaguardas dos direitos humanos e para a privacidade, valores que foram estabelecidos com muita luta.[9]

Propositalmente, o presente artigo buscou laborar com o neologismo (des)liberdade, buscando chamar atenção ao que se propõe: pensar no termo *desliberdade*, enquanto desigualdade política ou a partir do pressuposto de não haver (verdadeira) igualdade sem liberdade. Ou seja, demonstrar a importância do não aderir a ótica equivocada de que a igualdade proposta somente possa ser alcançada com absoluta/irrestrita liberdade no controle dos meios digitais para os fins do controlador, ou seja, com *desliberdade*.

A privacidade, proteção dos dados pessoais e à informação, como direitos fundamentais e subjetivos do cidadão, representam verdadeiros pilares ao Estado Democrático de Direito e a efetivação deles requer amplo envolvimento social.[10] Cabe ressaltar que a Lei nº 13.709/18 não foi formatada especificamente para situações do período de pandemia e, inclusive, na questão das multas dependerá da estruturação da autoridade nacional de dados (processo com previsão para se completar em 2021), por isso cautelas são necessárias em respeito a direitos elementares da pessoas. Frente a possibilidade de um estado de vigilância, cada vez mais globalizado e com múltiplos interesses mercadológicos e pessoais em jogo - problemática que nos desafia constantemente -, torna-se imprescindível para formulação de políticas públicas (e há competência federal, estadual e municipal), em que sejam utilizados dados pessoais. Contudo, tal deve ocorrer em prol do inerente interesse público, garantindo-se essa dimensão (pública) não exclusivamente governamental, bem como, estendendo-se aos tutelandos a proteção da privacidade e a promoção ao acesso de informações sob a forma anonimizada.[11]

Observe-se que esta crise atual oferece uma oportunidade de demonstrar nossa humanidade compartilhada. Existem possibilidades fáticas de empreendermos esforços extraordinários para combater esta pandemia mantendo-se consistentes com os padrões de privacidade e aos pilares do Estado de Direito.[12] As decisões que os governos tomam agora para enfrentar essa crise irão moldar muito da realidade do mundo no futuro.

---

7 Recorrendo a analogia sobre a proteção de direitos fundamentais, mencionamos a expressão clássica de Frederic Bastiat quando disse: "Não é porque os homens promulgaram Leis que a Personalidade, a Liberdade, e a Propriedade existem. Pelo contrário, é porque a Personalidade, a Liberdade, e a Propriedade preexistem que os homens fazem Leis". (BASTIAT, Frédéric. *A lei.* LVM Editora. Edição do Kindle, posição 222, 2019, p. 18).

8 LAI, P. C.; WONG, C. M.; HEDLEY, A. J.; LEUNG, G. M.. "Spatial clustering of SARS in Hong Kong". *Hong Kong medical journal* = Xianggang Yi Xue Za Zhi, v. 15, Suppl 9, 2019, p.17-19.

9 MCDONALD, Sean Martin. *Ebola: A Big Data Disaster* - Privacy, Property, and the Law of Disaster Experimentation. CIS Papers, 2016.

10 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, p. 67-79, 1999.

11 BIONI, Bruno. Compreendendo o conceito de anonimização e dado anonimizado. *Cadernos Jurídicos,* São Paulo, ano 21, n.53, p.191-201, jan./mar., 2020. Disponível em: https://api.tjsp.jus.br/Handlers/Handler/FileFetch.ashx?codigo=118902

12 ALEUY, O. Alejandro; PITESKY, Maurice; GALLARDO, Rodrigo. Using multinomial and space-time permutation models to understand the epidemiology of infectious bronchitis in California between 2008 and 2012. *Avian diseases,* v.62, n.2, p.226-232, 2018. Disponível em: https://doi.org/10.1637/11788-122217-Reg.1.

2. DIREITOS FUNDAMENTAIS E DA PERSONALIDADE: A INTIMIDADE E A VIDA PRIVADA

O monitoramento das pessoas com utilização de meios eletrônicos (celular, tablet, etc.) e dados neles gerados ou mantidos é fonte de riscos, na medida em que se relaciona com a proteção de direitos fundamentais e os direitos da personalidade. A LGPD deixa explícita essa circunstância e volta-se para esse tipo de proteção. Como afirma Rony Vainzof:

> Outrossim, independentemente dos fundamentos da LGPD, que veremos na sequência, buscarem um equilíbrio na manutenção do desenvolvimento econômico e tecnológico de modelos de negócio inovadores, públicos ou privados, com a inviolabilidade de direitos constitucionais dos cidadãos, a parte final do art. 1º não deixa qualquer dúvida que o seu objetivo está intrinsecamente vinculado à proteção dos direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. E a utilização do verbo "proteger", no art. 1º, também demonstra a necessidade coerente que o legislador enxergou no titular dos dados como vulnerável em comparação com os agentes de tratamento.[13]

Nesse contexto, diante da coincidência entre diversos direitos fundamentais, especial atenção deve ser tributada para os da personalidade; entendidos estes como consistentes nos atributos inerentes a pessoa e assim ligados de forma permanente a ela.

Foi a partir da Segunda Guerra Mundial que houve a reconstrução dos direitos da personalidade, alçando a pessoa humana ao centro do ordenamento jurídico. Institui-se a personalidade como um metaprincípio da dignidade da pessoa humana, bem como, foi esta reconhecida como característica inata do ser humano[14], sendo-lhe indissociável, irrenunciável e pertencente à positivação dos direitos humanos no ordenamento jurídico. As atrocidades provocadas durante as guerras fizeram emergir a compreensão dos direitos fundamentais ligados a personalidade.

À título exemplificativo temos: os direitos à privacidade, à vida, à honra, à liberdade, dentre outros. Ou seja, são os direitos que possibilitam ao seu titular, promover a defesa do que lhe é próprio. Portanto, não se limitam ao contido em visão primeira encartada no Código Civil, consistente na aptidão que tem todo homem, por força da lei, de exercer seus direitos e contrair obrigações.[15]

Rubens Limongi França conceitua os direitos da personalidade como "faculdades jurídicas cujo objeto são os diversos aspectos da própria pessoa do sujeito, bem assim as emanações e prolongamentos".[16]

Neste sentido, Adriano de Cupis assevera que os direitos da personalidade são os "direitos subjetivos, cuja função, relativamente à personalidade, é especial, constituindo o mínimo necessário e imprescindível ao seu conteúdo".[17]

Destarte, os direitos da personalidade se vinculam com o ser humano e com os atributos que lhe são inerentes na condição de pessoa. Por isso, não podem lhe ser retirados, nem mesmo sob sua autorização, ou seja, são irrenunciáveis, de mesma forma, independem da chancela estatal no plano do direito positivo, embora deste se utilizem para sua implementação.

13 MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. LGPD: Lei geral de proteção de dados comentada, São Paulo: Thomson Reuters Brasil, 2019, p. 20.

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

15 PRADO, Luiz Régis. *Bem Jurídico-penal e Constituição.* 2. ed. São Paulo: Revista dos Tribunais, 1997, p.437.

16 FRANÇA, Rubens Limongi. *Manual de Direito Civil.* 2. ed., v.1, 1971, p.321 *apud* FACHIN, Antonio Zulmar. *A proteção jurídica da imagem.* São Paulo: Celso Bastos, 1999, p.28.

17 CUPIS, Adriano de. *Os direitos da personalidade.* Trad. Afonso Celso Furtado Rezende. Campinas: Romana, 2004, p.23-24.

Nesse contexto se observa a importância da proteção dos dados e informações que porventura sejam coletados das pessoas, fazendo-se referência que a Constituição Federal em seu art. 5° traz protege *à inviolabilidade da intimidade, da vida privada, da honra e da imagem* da pessoa, desaguando em indenização por danos materiais ou morais quando de sua violação.

E é nesse contexto, que cabe configurar o conceito de *direito à privacidade*[18], em sentido genérico e amplo, atraindo por meio desta terminologia todas as manifestações da esfera privada, íntima e da personalidade. Em suma, utilizar o termo privacidade de forma a abarcar em seu arcabouço, a intimidade e a vida privada. Observe-se, entretanto, que as terminologias apresentadas, não recepcionam de maneira compatível os conceitos que se procura alcançar (intimidade e vida privada) sob o prisma do direito digital e novas tecnologias. Com a revolução da tecnologia, houve no mundo uma factual modificação da realidade social, de modo que essa mutação penetrou em todas as esferas da vida humana, gerando novas relações a serem estudadas e reguladas pelo ordenamento jurídico.

Neste enredo, o uso da internet estabeleceu novas formas de intrusão à vida privada e intimidade dos indivíduos.[19] Através das redes sociais a disponibilização de informações privadas presumidamente passou a ser controlada pelo próprio usuário, seja para um grupo de amigos ou aberta ao público. No entanto, esta privacidade é relativa, pois ainda que os dados se encontrem restritivamente direcionados aos partícipes do grupo, há que se confrontar esta restrição, quando se observa e faz uma análise quanto ao local de armazenamento destas informações. Afinal, estas estão vinculadas em provedores externos, respaldadas por contratos de adesão[20], em grande maioria, extremamente abusivos conforme à legislação brasileira em termos de privacidade.[21] Detalhe: também é comum que violação da esfera privada não ocorra por ilícito de terceiro, mas sim, pelo próprio usuário que concorda em participar da utilização e a seu livre arbítrio digital, disponibiliza e/ou permite o compartilhamento.[22]

Numa visão da *práxis* jurídica, diante da influência da mídia, que, por vezes, viola direitos tidos como essenciais à pessoa humana, constitui-se um lastro que não se apaga facilmente com o decurso do tempo. No meio digital os dados seguem presentes o suficiente para usos diversos, seja para fornecer elementos no planejamento de serviços públicos, seja para fins irregulares. Sejam falsos ou verdadeiros, para finalidades lícitas ou ilícitas, os dados se mantêm, formando um histórico útil para objetivos de bem comum, ou até desvirtuadamente, servindo apenas para julgamento permanente pelo denominado "tribunal" da internet ou outros fins criminosos.

Vale a advertência contida na lição de Elimar Szaniawski temos que o *"direito à intimidade objetiva resguardar a vida íntima e privada das pessoas"* [23] Se é íntima e privada, quer dizer que o próprio indivíduo que as detém optou por não divulgar amplamente e apenas por razões de ordem pública (que podem acontecer em tempos de pandemia) é que se pode relativizar esses princípios, mas não de forma permanente.

Deste modo, a coleta, o manuseio e o armazenamento de dados (mesmo durante o enfrentamento da pandemia), além de observar o núcleo essencial dos direitos fundamentais e da personalidade, devem primar pela adequação, proporcionalidade e limites necessários para o atingimento das lícitas finalidades pretendidas, tudo no sentido de resultar em proteção da pessoa e da coletividade, tal como se discorrerá.

18 SILVA, J. A. *Curso de direito constitucional positivo.* 29. ed. São Paulo: Malheiros, 2007, p. 206.
19 DONEDA, D. *Da privacidade à proteção de dados pessoais*. São Paulo: Revista dos Tribunais, 2019.
20 Doc Sears*, Do we have to "trade off" privacy?,* Doc Sears, set. 2010.
21 MENDES, Laura Schertel. *Privacidade, proteção de dados e defesa do consumidor*: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014.
22 FERRETTI, L. *et al.* Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing. *Science,* v.368, n.641, 08 maio 2020, p.8.
23 SZANIAWSKI, Elimar. *Direitos da personalidade e sua tutela.* 2.ed. São Paulo: Revista dos Tribunais, 2005, p. 301.

3. DA PRÁTICA DE COLETA E TRATAMENTO DE DADOS À NIVEL GLOBAL

Até que as vacinas estejam amplamente disponíveis, as únicas abordagens de prevenção de infecção disponíveis são o isolamento, rastreamento de contato e quarentena, distanciamento físico-social, descontaminação e outras medidas de higiene. Para implementar as providências corretas no momento certo, é de crucial importância compreender as rotas e horários de transmissão, mas, ressalte-se, as informações de saúde são privadas e confidenciais por natureza, posto que revelam detalhes íntimos da vida de uma pessoa[24], e por isso sua coleta e processamento justificam que exista proteção abrangente na legislação.

No Brasil, a Lei Federal 13.979/2020[25], passou a determinar critérios para atuação do Ministério da Saúde, o que inclui realização compulsória de testes e a mobilização de forças ostensivas para o correto cumprimento de medidas de quarentena e isolamento social, o que veio envolver direitos constitucionais elementares como, locomoção, liberdade econômica, etc. em paralelo, convém ressaltar que a legislação reconhece o respeito à direitos humanos, dignidade e liberdade fundamentais, conforme estabelecido no Regulamento Sanitário Internacional produzido pela Organização Mundial da Saúde e recepcionado pelo Brasil, por intermédio do Decreto 10.212/2020.

O referido regulamento dedicou parte de sua criação à proteção de dados pessoais, inclusive, sensíveis conforme seu artigo 45, que dispôs que as informações de saúde devem ser mantidas em sigilo e processadas anonimamente mediante balizas de leis nacionais.

Tais preceitos estão em compatibilidade com a Lei Geral de Proteção de Dados (LGPD) e demais normas pertinentes (Marco Civil da Internet e Decreto 10.212/2020), que devem ser encaradas dentro dos parâmetros constitucionais que garantem, dentre outros direitos, a inviolabilidade dos direitos a vida, liberdade, à igualdade, segurança, propriedade, honra, liberdade de reunião.

Em mesmo sentido, uso de informações de saúde, mais sensíveis que variam do tipo sanguíneo, pré-condições médicas, informações genéticas, registros de temperatura são geralmente estritamente limitados para o uso. No entanto, durante uma crise de saúde pública, a questão não é se governos podem usar dados de saúde para ajudar aos problemas que surgiram, mas como isso pode ser feito sem perder de vistas a salvaguarda da privacidade e a dignidade individual ao máximo possível. Cabe referir, inclusive, que conforme conceituação já amplamente aceita, saúde não é apenas ausência de doença, mas sim bem estar físico e menta, de modo que a proteção dos direitos digitais também promove a saúde pública.[26] De acordo com o Comitê das Nações Unidas sobre Direitos Econômicos, Sociais e Culturais,

> O direito à saúde está intimamente relacionado e depende da realização de outros direitos humanos, conforme contidos na Carta Internacional de Direitos, incluindo os direitos à alimentação, moradia, trabalho, educação, dignidade humana, vida, não discriminação, igualdade, proibição da tortura, privacidade, acesso à informação e liberdade de associação, reunião e movimento. Esses e outros direitos e liberdades tratam de componentes integrais do direito à saúde.

24 GUANAES, P.; SOUZA, A.R., DONEDA, D.; NASCIMENTO, F.J.T. *Marcos legais nacionais em face da abertura de dados para pesquisa em saúde:* Dados pessoais, sensíveis ou sigilosos e propriedade intelectual. Rio de Janeiro: Fiocruz, 2018.

25 Lei n.13.979/2020. Dispõe sobre as medidas para enfrentamento da emergência de saúde pública de importância internacional decorrente do coronavírus responsável pelo surto de 2019. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/L13979.htm>. Acesso em: 17 setembro 2020.

26 DONEDA D.; ALMEIDA, B.A.; BARRETO, M.L. Uso e proteção de dados pessoais na pesquisa científica. *Revista Direito Público*, v.16, n.90, 2019, p.179-194.

No combate à COVID-19, cabe as autoridades, com confiança, ampararem-se em dados, incluindo os de saúde, com vistas a determinar o melhor curso de ação para mitigar a propagação do vírus e identificar quais medidas devem ser tomadas para proteger as pessoas e seus direitos durante e após a crise. Todavia, de modo inegociável, todas as medidas aplicadas devem ser transparentes, necessárias e proporcionais, sendo que as exceções devem restar explícitas e claras para as pessoas atingidas e para a sociedade como um todo.

Em análise de diferentes respostas de uma variedade de estados autoritários, híbridos e democráticos mostra que, de fato, a pandemia abriu o espaço para testar não apenas a resiliência da democracia, mas até que ponto irá a possibilidade do poder ser abusado e expandido no nome de proteger os cidadãos.[27] No mundo contemporâneo, pontos de dados onipresentes e ferramentas de vigilância digital podem facilmente exacerbar essas preocupações. A utilização de big data será crítica para o gerenciamento das medidas de enfrentamento da pandemia COVID-19, mas em relação a coleta e utilização de dados, os limites legais e éticos precisam ser respeitados.[28] Sabe-se que o uso de dados e algoritmos disponíveis digitalmente para previsão e vigilância[29] - por exemplo, para identificar pessoas que viajaram para áreas onde a doença se espalhou ou rastrear e isolar os contatos de pessoas infectadas - é de extrema importância na luta contra o alastramento do COVID-19.[30] É igualmente importante, no entanto, usar esses dados e algoritmos de forma responsável, inclusive atendo-se a uma perspectiva de longo prazo.

De maneira uniforme, governos e empresas devem aplicar a seguinte proteção de dados e princípios de privacidade: *(i) Limitação de finalidade e minimização de dados:* coleta de dados, uso, compartilhamento, armazenamento e outro processamento de dados de saúde devem ser limitados ao estritamente necessári o para a luta contra o vírus. Uma pandemia não é justificativa para coletar dados extensos e desnecessários; *(ii) Limitação de acesso e segurança de dados*: o acesso aos dados de saúde deve ser limitado a quem precisa de informações para conduzir o tratamento, pesquisar e resolver de outra forma a crise. As informações devem ser armazenadas de forma segura, em um banco de dados separado; *(iii) Retenção de dados e pesquisas futuras:* Os dados processados em resposta à crise devem ser mantidos apenas durante a crise. Posteriormente, a maioria dos dados de saúde deve ser apagada, embora algumas informações não identificáveis possam ser mantidas para fins históricos e de pesquisa. Essas informações devem ser acessíveis e usadas apenas para esses fins de interesse público; *(iv) Vedação ao uso com finalidades lucrativas:* Em nenhuma circunstância os dados de saúde devem ser vendidos ou transferidos à terceiros que não trabalhem no interesse público.

Aonde ocorrem crises de saúde pública e não importa se os países têm leis de proteção de dados e privacidade em vigor, essas diretrizes básicas devem ser aplicadas, sendo eventuais exceções restritas ao momento emergencial com salvaguardas relacionadas

27 Organisation for Economic Co-operation and Development (Org.). New mobile applications for COVID-19 "tracking" are also being launched. 2020. Disponível em: http://www.oecd.org/coronavirus/policy-responses/tracking-and-tracing-covid-protecting-privacy-and-data-while-using-apps-and-biometrics 8f394636/#section-d1e108. Acesso em: 08 set. 2020. Organisation for Economic Co-operation and Development (Org.). New mobile applications for COVID-19 "tracking" are also being launched. 2020. Disponível em: http://www.oecd.org/coronavirus/policy-responses/tracking-and-tracing-covid-protecting-privacy-and-data-while-using-apps-and-biometrics 8f394636/#section-d1e108. Acesso em: 08 set. 2020.

28 RODOTÁ, S. *A vida na sociedade da vigilância:* a privacidade hoje. Rio de Janeiro: Renovar; 2008.

29 LANDAU, Susan. *Location Surveillance to Counter COVID-19:* Efficacy Is What Matters. 25 mar. 2020. Disponível em: https://www.lawfareblog.com/location-surveillance-counter-covid-19-efficacy-what-matters. Acesso em: 7 set. 2020.

30 ALIMADADI, Ahmad; ARYAL, Sachin; MANANDHAR, Ishan; MUNROE, Patricia B.; JOE, Bina; CHENG, Xi. "Artificial intelligence and machine learning to fight Covid-19". *Physiological genomics*, v. 52, n.4, 2020, p.200-202. Disponível em: https://doi.org/10.1152/physiolgenomics.00029.2020.

a capacidade aumentada de processar dados.[31]

Em mesma frente, deve ser absolutamente vedada a divulgação de dados identificáveis sobre pacientes infectados e curados. Os relatórios e seus elementos não devem revelar informações pessoais sobre pacientes. Especificamente, quaisquer informações identificáveis, especialmente nome, data de nascimento ou endereço, sobre pessoas afetadas pelo vírus. não devem ser compartilhadas com pessoas físicas ou jurídicas alheias a finalidade legitimada. O compartilhamento e a publicidade dos dados coloca os indivíduos em risco e a ordem pública em perigo, pois, inclusive, entes privados estão buscando maneiras de monetizar esses dados, o que depõe contra os princípios de privacidade. Havendo coleta de informações pessoais confidenciais, os governos devem envolver especialistas da comunidade de privacidade e saúde para ajudar a desenvolver e implementar salvaguardas sobre o uso de dados, especialmente em países onde exista carência de instituições robustas de regulação da privacidade e proteção de dados. Importante haver cuidados especiais com as comunidades em risco de marginalização, incluindo mulheres (principalmente as meninas), pessoas com deficiência, grupos indígenas, os pobres, pessoas LGBTQ, minorias religiosas e étnicas e outros tipos de vulneráveis, que muitas vezes sofrem o impacto da discriminação e não têm acesso a cuidados de saúde. O zelo por estes, inclusive com direito de terem vez e voz nas consultas quando da criação de normas e instituições específicas para salvaguardas eficazes.[32] E nem mesmo na pandemia cabe reduzir a transparência, pois embora esta, por si só, seja insuficiente para proteger a privacidade individual, deve restar claro para as pessoas o que acontecerá com seus dados, seja na situação de crise na saúde, seja voltando a normalidade. As medidas tomadas em resposta a pandemias devem adequadas para garantir que as respostas sejam benéficas para resolver a crise sem sacrificar a privacidade individual.

4. PRIVACIDADE VERSUS DIREITO À SAUDE: UM TROCA DESLEAL

Quando as grandes empresas de tecnologia[33] prestam serviços públicos em nome dos governos, elas geram não apenas dados valiosos, mas também excedentes políticos que podem explorar posteriormente para garantir contratos governamentais. Em outra frente, quando governos fazem parceria com empresas de tecnologia para tirar proveito de sua vasta coleta de dados e infraestruturas de processamento, adquirem excedente de governança que permite a redistribuição das infraestruturas de vigilância em aplicações de policiamento punitivo. Assim, os excedentes advindos dessas ferramentas permitem a mercantilização e o abuso ao longo do tempo. Governos e empresas de tecnologia há muito se mostram como lobos em pele de cordeiro no que diz respeito à privacidade: prometendo-a, ao mesmo tempo em que podem conduzir uma vigilância ampla e ilícita, sempre sob o manto de algum argumento aparentemente válido.

É um dilema atroz e injusto aceitar o *trade-off* entre privacidade e saúde nesses termos, e só serve para nos conduzir em direção a um estágio de vigilância ampliada, ao mesmo tempo em que confere validade para determinadas estruturas de mercados. A esperança de que as extensas infraestruturas de vigilância público-privadas do mundo possam dar

31 CORDEIRO, A. Barreto Menezes. *Direito da Protecção de Dados* - À luz do RGPD e da Lei n.º 58/2019. Coimbra: Almedina, 2020, p. 39.

32 HARARI, Yuval Noah. *The world after coronavirus.* Disponível em: https://www.ft.com/content/19d90308-6858-11ea-a3c9-1fe6fedcca75. Acesso em: 27 ago. 2020.

33 AYYOUBZADEH, Seyed-Mohammad; AYYOUBZADEH, Seyed-Mehdi; ZAHEDI, Hoda; AHMADI, Mahnaz; KALHORI, Sharareh R. Niakan. "Predicting Covid-19 incidence through analysis of Google trends data in Iran: Data mining and deep learning pilot study". *JMIR Public health and surveillance,* v. 6, n. 2, e18828. Disponível em: https://doi.org/10.2196/18828.

uma reviravolta em direção a medidas de saúde pública equitativas e democráticas, na atual conjuntura se revela uma utopia.

Vale ressaltar, esses projetos são artifícios que funcionam como natural para o enquadramento dos debates "privacidade vs. saúde; privacidade vs. segurança", etc. Governos e entidades corporativas estão com a possibilidade de usar a crise para aumentar as infraestruturas de vigilância biométrica, mas que poderá se tornar dispositivos permanentes usados para fins invasivos muito além de seu desiderato original de saúde pública.

Observe-se, inicialmente, o quão importante é ressaltar que essas parcerias tecnológicas público-privadas terão potencial de serem excludentes, na medida em que práticas punitivas de aplicação da lei, conforme sua utilização, podem atingir desproporcionalmente as minorias e aos pobres. E é evidente que com a pandemia, os agentes de aplicação da lei usam as tecnologias de quem dispõem.

Assim, aceitar a ideia de que a resposta efetiva à pandemia é principalmente um problema de implementação técnica para ajudar a fiscalização, na verdade obscurece e dissimula o debate necessário sobre como garantir as condições materiais que as pessoas exigirão para cumprir ordens prolongadas de distanciamento social, posto que afetam seu bem-estar social. A combinação entre a infraestrutura digital de propriedade privada, com sua aplicação pelo Estado, inclusive, pode ter consequências econômicas, à medida que governos e entidades corporativas usem a crise para extrair e/ou mercantilizar dados pessoais[34]. Na medida em que as infraestruturas de dados e comunicações se tornam recursos essenciais no combate ao vírus, as entidades que têm (ou afirmam ter) capacidade para alavancar essas infraestruturas podem utilizar a sua posição para obter ganhos econômicos ou políticos desmedidos. Nessas condições, sacrificar a privacidade pela saúde significa ceder mais controle a governos e empresas de tecnologia que já ganharam poder indevido por meio dos meios tecnológicos que dispõem.

Reconhecer isso é essencial para nos reorientar a essa escolha, um falso dilema, desnecessário para uma nova agenda de reformas. Precisamos redesenhar nossos mundos sóciotécnicos em resposta ao que a crise da saúde expôs sobre a realidade pré-pandêmica de nossas instituições sociais e políticas: suas estruturas arraigadas de desigualdade e austeridade que exacerbaram a vulnerabilidade de tantos em nossa sociedade. A história da COVID-19 não é apenas a de uma nova pandemia ou de novas ameaças à privacidade, mas também de uma falha institucional mundial. Na visão de Boaventura de Souza Santos ela é um verdadeiro oximoro, mas revelador de uma condição sistêmica, uma crise maior que tem sido permanente devido ao modelo que está a prevalecer socialmente.[35]

A precipitação e desastrosa resposta dos EUA à pandemia do coronavírus expôs as falhas das lógicas de mercado que pressupõem o bem-estar social no que é lucrativo e não no que é socialmente valioso e de governos que ignoram os avisos sobre nossa incapacidade de lidar com uma pandemia. Como advertiu Yuval Noah Harari[36], realmente o mundo está a carecer de autênticos líderes (sejam pessoas, sejam países), mas enquanto restar um infectado, a humanidade não estará completamente a salvo desse flagelo.

No Brasil, o Supremo Tribunal Federal, derrubou uma ordem governamental que obrigava as empresas de telecomunicações a fornecerem acesso às informações de usuários, o que atingiria 200 milhões de cidadãos do país. O objetivo esposado foi de viabilizar paro

34 Algo semelhante as tentativas de acumular e aumentar o estoque de máscaras e desinfetantes para as mãos.
35 SANTOS, Boaventura de Sousa. *A cruel pedagogia do vírus* (Pandemia Capital) (p. 4, posição 14). Boitempo Editorial. Edição do Kindle, 2020.
36 HARARI, Yuval Noah. *Na batalha contra o coronavírus, faltam líderes à humanidade* (Breve Companhia). Companhia das Letras. Edição do Kindle. 2020.

o governo a realização de entrevistas por telefone e assim avaliar a resposta econômica à pandemia COVID-19[37]. No processo que negou autorização, a decisão estabeleceu que a proteção de dados é um direito fundamental. No entanto, tanto o governo federal brasileiro quanto pelo menos 14 de seus 27 governos estaduais, como parte da resposta ao COVID-19, procuraram de alguma forma, coletar dados dos brasileiros. Esse tipo de busca que pode revelar também em relação as interações sociais e movimentos recentes de pessoas infectadas, devem ter como pré-requisito obrigatório a necessidade de consentimento. O direito à privacidade não perece nem mesmo em nome da vigilância de doenças, pois isso pode alimentar a desconfiança e, em última análise, revelar-se desvantajosa.[38]

Em se tratando vigilância há que se preocupar com o fato de que as normas estabelecidas e as práticas e ferramentas, tendem a se consolidar. E quem pode dizer quando isso vai acabar? Nos Estados Unidos, se lida com a escalada no padrão de vigilância, algo que supostamente deveria ser temporário, mas que autorizado há quase 20 anos atrás (após o 11 de setembro) ainda se mantém e com tendência de ampliação. Note-se que as ferramentas que construídas costumam criar dependência que molda o futuro em relação as políticas relacionadas a dados e práticas de vigilância.

Em vistas de sintetizar o raciocínio aqui aduzido, pertinente abordarmos as conclusões feitas durante a pandemia por Yuval Noah Harari, em tradução livre aduz:

> Pedir às pessoas que escolham entre privacidade e saúde é, na verdade, a verdadeira raiz do problema. Porque esta é uma escolha falsa. Podemos e devemos ter privacidade e saúde. Podemos escolher proteger nossa saúde e interromper a epidemia de coronavírus, não instituindo regimes de vigilância totalitários, mas sim empoderando os cidadãos. (HARARI, 2020).[39]

Por certo, para responder à crise do COVID-19 e aos colapsos sociais mais amplos que nos trouxeram até aqui, será necessário canalizar esses insights duramente conquistados para reequipar várias instituições, no sentido da proteção das pessoas e de condutas democráticas e igualitárias. Nossas infraestruturas de dados não devem ser exceção, conforme se exemplificará.

5. RASTREAMENTO E GEOLOCALIZAÇÃO: OS RISCOS IMINENTES

Os dados de localização são altamente reveladores. Simplesmente seguindo o movimento de uma pessoa com base nos dados de localização de um smartphone[40], você pode deduzir seu endereço residencial e local de trabalho, mapear sua interação com outras pessoas, identificar suas consultas médicas, inferir sua situação socioeconômica e muito mais. Sem salvaguardas adequadas, as ferramentas de rastreamento e localização geográfica estão permitindo a vigilância onipresente.

No contexto de uma crise de saúde pública, como o surto de COVID-19, governos querem contar com o rastreamento da localização para mapear a evolução do vírus e planejar suas respostas. Mas esse rastreamento traz uma série de preocupações, a começar pelo

37 Supremo Tribunal Federal. MC - ADI 6387/DF, Rel. Min. Rosa Weber. CFOAB x Presidente da República. Disponível em: <http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADI6387MC.pdf>. Acesso em: 21 maio 2020.

38 BIONI, Bruno Ricardo. *Proteção de dados pessoais:* a função e os limites do consentimento. 2. ed. Rio de Janeiro: Grupo Editorial Nacional, 2020.

39 FINANCIAL TIMES. Yuval Noah Harari: the world after coronavírus. Disponível em: https://www.ft.com/content/19d90308-6858-11ea-a3c9-1fe6fedcca75/. Acesso em: 07 set. 2020.

40 BENGTSSON, Linus; GAUDART, Jean; LU, Xin; MOORE, Sandra; WETTER, Erik; SALLAH, Kankoe; REBAUDET, Stanislas; PIARROUX, Renaud. "Using mobile phone data to predict the spatial spread of cholera". *Scientific reports,* v. 5, n. 1, 2015. Disponível em: https://doi.org/10.1038/srep08923.

fato de que o rastreamento é dos telefones das pessoas, não do vírus. Em segundo lugar, mesmo os chamados dados de localização anônimos podem ser facilmente reidentificados; um estudo de 2013 mostrou que as pessoas podiam ser reidentificadas a partir de apenas quatro pontos de dados. Em terceiro lugar, a localização geográfica pode não ser útil em razão de que as pessoas podem dirigir, caminhar, pegar o metrô ou trabalhar no 10º andar de um prédio de 30 andares. Então, saber a localização geográfica de uma pessoa fornece apenas informação parcial, mas ainda assim sacrifica a privacidade pessoal. Outro detalhe: em respostas humanitárias como a que se menciona, os usos anteriores de registros telefônicos e dados de localização se mostraram ineficientes e ineficazes.[41] Assim, usar a geolocalização para ajudar a resolver o problema da disseminação do vírus deve ser conduzida de uma maneira que respeite direitos, que promova a confiança no governo e proteja a segurança e proteção individual, dado o risco elevado de vir a simplesmente redundar em um processo de vigilância em massa patrocinada pelo Estado; uma tentação autoritária que não pode contaminar países democráticos.

Em uma sociedade que rotineiramente pisoteia os direitos humanos, como a China, medidas diretas de coleta de dados são simplesmente parte do caminho. Taiwan usa monitoramento de rede móvel ativa para impor quarentena residencial para indivíduos recém-chegados ou em risco. As autoridades públicas são alertadas se o dispositivo móvel de um indivíduo estiver ativo fora de sua casa. Isso pressupõe que haja uma ligação documentada entre a identidade de cada indivíduo, seu número de telefone e seu endereço residencial, que inclui informações sobre coabitantes.[42] Para evitar que aqueles colocados em quarentena domiciliar ilidam as medidas, as autoridades públicas ligam para o número - supostamente duas vezes por dia - para assegurar que essas pessoas não abandonem seus dispositivos móveis e se aventurem para fora de casa.

Na África do Sul, os provedores de serviços de telecomunicações, de acordo com o Ministro das Comunicações, Telecomunicações e Serviços Postais, concordaram em compartilhar os dados de localização dos clientes com o governo[43], tudo sem deixar claro se são apenas dados de localização dos casos confirmados ou de toda a população. O ministro do referido país declarou que "a indústria concordou coletivamente em fornecer serviços de análise de dados para ajudar o governo a alcançar a luta contra o vírus".[44]

Em mesmo sentido, na Coreia do Sul o governo rastreia e publica dados online detalhando a localização de pessoas confirmadas e suspeitas de estarem infectadas pelo vírus. Ao fundir bancos de dados existentes, esses novos conjuntos fornecem rastreamento dinâmico por meio de imagens de CFTV, incluindo não apenas dados da localização, mas também históricos de utilização do cartão de crédito. O material publicado online inclui uma riqueza de informações, como detalhes sobre quando as pessoas saíram para trabalhar, se usaram máscaras no metrô, o nome das estações onde trocaram de trem, os bares de karaokê que frequentavam e os nomes das clínicas onde foram testados.[45]

Semelhantes práticas acontecem na União Europeia, onde empresas de

41 CIS-India. *Ebola:* A big data disaster, 2016. Disponível em: https://cis-india.org/papers/ebola-a-big-data-disaster. Acesso em 12 set. 2020.
42 Reuters. *Taiwan's new 'electronic fence' for quarantines leads wave of virus monitoring,* 2020. Disponível em: https://www.reuters.com/article/us-health-coronavirus-taiwan-surveillanc-idUSKBN2170SK. Acesso em: 12 set. 2020.
43 Business Insider SA. South Africa will be Tracking Cellphones to Fight the Covid-19 Virus. 2020. Disponível em:https://www.businessinsider.co.za/south-africa-will-be-tracking-cellphones-to-fight-covid-19-2020-3. Acesso em: 12 set. 2020.
44 The New York Times. In Coronavirus Fight, China Gives Citizens a Color Code, With Red Flags, 2020. Disponível em: https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html. Acesso em: 12 set. 2020.
45 The New York Times. As Coronavirus Surveillance Escalates, Personal Privacy Plummets, 2020. Disponível em: https://www.nytimes.com/2020/03/23/technology/coronavirus-surveillance-tracking-privacy.html. Acesso em: 12 set. 2020.

telecomunicações e autoridades públicas estão firmando acordos para compartilhar dados de localização.[46] Até agora, há pouca transparência sobre a quantidade de dados compartilhados e qual será a duração desses acordos, que muitas vezes podem ser considerados extralegais (baseados unicamente na excepcionalidade da atual conjuntura). Também não está explícito se as empresas estão fornecendo registros de metadados ou permitindo que governos conduzam monitoramento de pessoas em tempo real. Como exemplo, cita-se que na Bélgica, as empresas de telecomunicações, incluindo Orange e Proximus, concordaram em compartilhar "partes de seu banco de dados" para ajudar as autoridades a combater o surto de coronavírus.[47] E na Alemanha, a Deutsche Telekom está fornecendo parte de seus dados de localização para a Agência Federal de Prevenção de Doenças para ajudar a conter a pandemia. Além dos governos nacionais, a Comissão Europeia solicitou metadados agregados das operadoras de telecomunicações para "rastrear a propagação do vírus" e determinar onde a necessidade de suprimentos médicos é mais urgente.[48]

Na América do Sul, em especial na Argentina, um jornal publicou informações pessoais de pessoas infectadas, indicando sua idade, para onde haviam viajado, em que hospital foram atendidas e muito mais. Depois que essa publicação foi notada e criticada pelo público, eles posteriormente tornaram os nomes indisponíveis.[49] A semelhança, o Instituto Nacional de Saúde do Peru desenvolveu uma plataforma onde as pessoas podem consultar os relatórios de saúde de pacientes que foram testados para COVID-19, bastando inserir o número do próprio documento de identidade nacional. E, detalhe: por alguns dias, esse tipo de informação ficou, portanto, acessível ao público, não se limitando ao paciente. Depois de receber críticas, as autoridades nacionais do referido país incluíram um segundo autenticador (no caso, para se conectar à plataforma, um código baseado em SMS agora é necessário).[50]

Esses procedimentos vão na linha de ampliação da utilização de dados, prática disseminada nos Estados Unidos, país no qual pesquisadores estão usando dados do Facebook, como forma coletar o histórico de localização e desenvolver mapas com dados de localização agregados e não identificados. Este tipo de iniciativa apresenta riscos significativos à privacidade e proteção de dados, pois pressupõe que na luta contra a coronavírus, os usuários do Facebook concordam especificamente em ser rastreados pela plataforma.[51]

Entretanto, ela oferece riscos evidentes. A guisa de exemplo, menciona-se na Índia, pelo menos dois governos estaduais - incluindo o estado de Karnataka, que abriga o centro de tecnologia de Bangalore - carregaram arquivos PDF online com nomes, endereços residenciais e histórico de viagens de pessoas solicitadas em quarentenas COVID-19. A informação ficou acessível por todos.[52] E há casos como o do cidadão norte-americano Frank King que fez um

46 European Data Protection Board. Processing of personal data in the context of the COVID-19 outbreak, 2020. Disponível em: https://edpb.europa.eu/news/news/2020/statement-edpb-chair-processing-personal-data-context-covid-19-outbreak_en. Acesso em: 12. set. 2020.
47 Le Soir. Coronavirus: le cabinet De Block dit «oui» à l'utilisation des données télécoms, 2020. Disponível em: https://plus.lesoir.be/286535/article/2020-03-12/coronavirus-le-cabinet-de-block-dit-oui-lutilisation-des donnees-telecoms. Acesso em: 12. Set. 2020.
48 Politico. Commission tells carriers to hand over mobile data in coronavirus fight, 2020. Disponível em: https://www.politico.eu/article/european-commission-mobile-phone-data-thierry-breton-coronaviruscovid19/. Acesso em: 12. set. 2020.
49 Asociación para el Progreso de las Comunicaciones. Ecuador: Las tecnologías de vigilancia en contexto de pandemia no deben poner en riesgo los derechos humanos, 2020. Disponível em: https://www.apc.org/es/pubs/ecuador-las-tecnologias-de-vigilancia-en-contexto-de-pandemia-no-deben-poner-en-riesgo-los. Acesso em: 12. set. 2020.
50 Perú. Debilidades de plataforma del Ministerio de Salud exponen información de pacientes COVID-19, 2020. Disponível em: https://saludconlupa.com/noticias/peru-debilidades-de-plataforma-del-ministerio-de-salud-pueden-exponer-informacion-clinica-de-pacientes-covid-19/. Acesso em: 12. set. 2020.
51 Protocol. Facebook data can help measure social distancing in California, 2020. Disponível em:https://www.protocol.com/facebook-data-help-california-coronavirus. Acesso em: 12. set. 2020.
52 Bangalore Mirror. Government publishes details of 19,240 home-quarantined people to keep a check, 2020. Disponível em: https://bangaloremirror.indiatimes.com/bangalore/others/government-publishes-details-of-19240-home-quarantined-people-to-keep-a-check/articleshow/74807807.cms. Acesso em: 12. set. 2020.

cruzeiro no Camboja, onde foi identificado por engano como um transportador COVID-19. Mesmo que os resultados dos testes do Sr. King tenham sido corrigidos e todos os passageiros do cruzeiro estivessem determinados como saudáveis, ao retornar aos EUA, ele recebeu ameaças de morte e ataques pessoais, online e offline, nas semanas seguintes.[53] Também nos Estados Unidos, mais de 2.000 profissionais de emergência médica da Universidade da Califórnia, do San Francisco Medical Center e do Zuckerberg San Francisco General Hospital participarão de um estudo que envolve o uso de um anel inteligente na tentativa de identificar as pessoas que têm COVID-19 mais cedo. Os anéis serão dados a profissionais de saúde de emergência que entrarem em contato com pacientes que possam ter COVID-19. O anel, que os trabalhadores terão que usar por três meses, coleta informações de saúde, como frequência cardíaca e respiratória das pessoas e mudanças na temperatura corporal. Não foi comprovado que o dispositivo detecta COVID-19, mas os dados de saúde dessas pessoas ficaram armazenados.[54]

No Brasil, não descolado dessas iniciativas comuns em outros países, vários governos dos três níveis (federal, estadual e municipal) se valeram de soluções de geolocalização, conforme a parceria da Prefeitura de Recife[55] com a empresa In Loco[56], que incluiu acompanhamento por geolocalização de smartphones, de forma coletiva, e envolvendo o isolamento social por bairros. Por sua vez, o Estado de São Paulo, de acordo com comunicado do governo,[57] o Sistema de Monitoramento Inteligente de São Paulo denominado (Simi-SP) surgiu a partir de parceria entre o governo estadual e as operadoras de telefonia Vivo, Tim, Oi e Claro, que usa dados digitais para medir a adesão à quarentena em todo o Estado, sendo que também envia mensagens de alerta para regiões com maior incidência da COVID-19.

Note-se que o rastreamento de contatos é uma estratégia de controle de doenças que requer interação e engajamento, tanto em nível individual, quanto comunitário. Encontrar indivíduos infectados, identificar aqueles que foram expostos ao vírus e prevenir que os infectados e potencialmente infectados transmitam a doença é objetivo de saúde pública. Já o rastreamento de contatos quando vai além dos propósitos de modificação das condições ambientais ou de promoção de comportamentos saudáveis, extrapola seus objetivos meritórios.

6. PARCERIAS PÚBLICO-PRIVADAS: APPS, WEBSITES E SERVIÇOS USADOS EM RESPOSTA AO COVID

Em qualquer crise pública, a solidariedade entre todos os atores da sociedade é necessária e desde o início da crise, governos e empresas de tecnologia têm trabalhado juntos para desenvolver soluções tecnológicas para combater o surto de COVID-19. Desde a coleta de dados, rastreamento de movimentos de cidadãos infectados, disseminação de

53 The New York Times. What It's Like to Come Home to the Stigma of Coronavirus, 2020. Disponível em:https://www.nytimes.com/2020/03/04/us/stigma-coronavirus.html. Acesso em: 12. set. 2020.

54 The Verge. New study aims to use health data from a smart ring to identify coronavirus symptoms, 2020. Disponível em: https://www.theverge.com/2020/3/23/21191225/coronavirus-smart-ring-oura-ucsf-san-francisco-general-hospital-tempredict. Acesso em: 12. set. 2020.

55 Prefeitura da Cidade de Recife. Prefeitura do Recife usa tecnologia como aliada na contenção do novo coronavírus. 24 mar. 2020. Disponível em: http://www2.recife.pe.gov.br/noticias/24/03/2020/prefeitura-do-recife-usa-tecnologia-como-aliada-na-contencao-do-novo-coronavirus. Acesso em: 12 set. 2020.

56 IN LOCO. Política de Privacidade: In Loco x COVID-19. 27 mar. 2020. Disponível em: https://www.inloco.com.br/pt/privacy-covid-19. Acesso em: 12. set. 2020.

57 Governo do Estado de São Paulo. Governo de SP apresenta Sistema de Monitoramento Inteligente contra coronavírus. 9 abr. 2020. Disponível em https://www.saopaulo.sp.gov.br/noticias-coronavirus/governo-de-sp-apresenta-sistema-de-monitoramento-inteligente-contra-coronavirus. Acesso em: 12 set. 2020.

alertas de saúde pública e monitoramento do paradeiro do público em geral, o setor privado está oferecendo uma infinidade de soluções tecnológicas.

Em particular, a crise em curso destaca o quanto o público e as autoridades públicas dependem das empresas de tecnologia para funcionar: desde fornecer acesso de banda larga a permitir que as pessoas acessem serviços públicos, a aplicativos de diagnóstico. Mas, sem salvaguardas adequadas para direitos humanos, fundamentais e da personalidade, as soluções tecnológicas apresentam muitos riscos. Contando com empresas privadas, os governos podem aumentar os poderes das plataformas dominantes e assim deixarem espaço para a monetização de informações de saúde, bem como, legitimar serviços invasores de privacidade. Convém ressaltar que várias empresas conhecidas por possibilitar violações de direitos humanos estão oferecendo publicamente, produtos para responder ao COVID-19, conforme abordado também na obra de Carlos Luiz Strapazzon[58], os quais poderão ser reaproveitados para vigilância em massa assim que a crise terminar.

O setor de tecnologia tem um papel importante a desempenhar, contribuindo no enfrentamento desta crise. No entanto, o histórico medíocre de direitos humanos de longa data da maioria das empresas de tecnologia, em particular na área de privacidade e proteção de dados, é um desafio significativo.

Na Colômbia, por exemplo, um aplicativo antigo foi reaproveitado e renomeado como CoronApp para fornecer informações sobre o vírus. Para funcionar, o aplicativo solicita uma grande quantidade de informações pessoais, tais como dados sobre etnia e não há transparência sobre quem tem acesso a esses dados e como eles podem ser usados.[59]

Na Guatemala, o governo lançou um aplicativo oficial para informar as pessoas sobre o COVID-19, chamado Alerta Guate. Para baixar o aplicativo, os usuários devem permitir o acesso aos dados de localização, ao microfone do telefone e a fornecer um endereço de e-mail ou número de telefone. [60]

Já na Tunísia, a Enova Robotics assinou um acordo com o Ministério do Interior para começar a operar robôs PGuard. Esses robôs serão equipados com um conjunto de câmeras infravermelhas e usados para impedir as pessoas de sair de suas casas. Não há informações sobre onde esses robôs serão implantados, quais informações eles coletarão, por quanto tempo eles manterão os dados e quem terá acesso a eles.[61]

Na China, aplicativos como o Alipay e o WeChat sinalizaram indivíduos de alto risco, que foram colocados em quarentena ou impedidos de entrar em espaços públicos. À medida que a normalidade retorna à região, as pessoas são obrigadas a obter uma "autorização verde" desses aplicativos para poder voltar à vida pública e se mover livremente.

Também na China, empresas como a SenseTime afirmam que seu software de detecção de temperatura sem contato foi implantado em Pequim, Xangai e Shenzhen. A empresa também afirma ter uma ferramenta de reconhecimento facial. Embora as câmeras de reconhecimento facial sejam comuns na China, essas câmeras estão sendo atualizadas

58 STRAPAZZON, Carlos Luiz; INOMATA, Adriana. Restrições, Privações e Violações de Direitos Constitucionais Fundamentais. *Revista Eletrônica de Direito do Centro Universitário Newton Paiva,* Belo Horizonte, n.32, p.85-104, maio/ago. 2017, p.100. Disponível em: https://revistas.newtonpaiva.br/redcunp/wp-content/uploads/2020/05/N.32-06.pdf. Acesso em: 13 dez. 2020.

59 Fundación Karisma. CoronApp, una barrera para el acceso a información pública y una pesadilla para la privacidad, 2020. Disponível em: https://stats.karisma.org.co/coronapp-inscolombia. Acesso em: 12 set. 2020.

60 La Hora. Sandoval sobre Alerta Guate: "Quien la quiera descargar lo puede hacer", 2020. Disponível em: https://lahora.gt/sandoval-sobre-alerta-guate-quien-la-quiera-descargar-lo-puede-hacer/. Acesso em: 12 set. 2020.

61 African Manager. A first in Tunisia: Pguard, the security robot to report violations, 2020. Disponível em: https://africanmanager.com/une-premiere-en-tunisie-pguard-le-robot-de-securite-pour-signaler-les-infractions. Acesso em: 12 set. 2020.

para maior precisão e detecção de temperatura.[62]

Cingapura tem um aplicativo chamado Tracetogether.[63] Ele permite que as pessoas compartilhem voluntariamente suas informações e rastreia outras pessoas com quem elas entram em contato via bluetooth. Se algum dos usuários do aplicativo contratar COVID-19, todos os usuários que entrarem em contato com essa pessoa serão notificados, juntamente com o governo. Também não há transparência sobre quem pode ter acesso a essas informações.

E em exemplo deplorável de falta de *compliance*, o infame Grupo NSO está explorando a crise global e lançando seus serviços de rastreamento para governos em todo o mundo. O software de *hacking* construído pela empresa foi implicado em inúmeras violações de direitos humanos, talvez mais notavelmente no assassinato de Jamal Khashoggi. O aplicativo (alegadamente testado em cerca de uma dúzia de países), leva duas semanas de informações de rastreamento de telefone celular de uma pessoa infectada e, em seguida, combina essas informações com os dados de localização coletados por empresas nacionais de telefonia móvel. O objetivo é identificar pessoas que estiveram nas proximidades do paciente por mais de 15 minutos e, portanto, poderiam ser vulneráveis ao contágio, mas nada é confiável se considerando o histórico do grupo NSO.[64]

É inerente a fluidez conceitual das noções de bem comum, interesse público e necessidades coletivas, tudo aliado a dificuldade de se ponderar e aplicar proporcionalidade entre direitos de igual status constitucional, no caso, à privacidade e à saúde pública. Nesse sentido, revela-se um dever jurídico de governos atenderem aos referidos valores constitucionais, como forma de, na busca da máxima otimização dos melhores interesses em jogo, protegerem, tanto o interesse coletivo, quanto o das pessoas individualmente consideradas, ambas razões primordiais para a justificação de existência do Estado.

7. CONCLUSÃO

O mundo está enfrentando uma crise de saúde pública que as gerações atuais não conheciam. E as respostas adotadas pelos governos para combater o COVID-19 terão um impacto além desta emergência, pois soluções meramente imediatistas costumam não defender os direitos humanos no médio e longo prazo. Dados e tecnologia serão componentes essenciais na luta contra o COVID-19, mas a questão problemática reside na possibilidade de governos acabarem usando dados e tecnologia, tanto para ajudar a combater o vírus, quanto para outros fins menos nobres. A mensagem deve ser simples: proteger os direitos digitais das pessoas também promove a saúde pública em seu sentido amplo; e sem que se precise de vigilância abusiva e ilícita.

Saliente-se três vetores para serem seguidos. Primeiro, devemos ir além dos indivíduos como *locus* de controle sobre os dados. Assim como a pandemia expôs o quão interconectados estamos em termos de saúde, também veio mostrar o quão interconectados estamos em termos de privacidade: quando se trata de pandemia e privacidade, os indivíduos que tomam decisões por si próprios, não são habilitados para produzir os melhores resultados coletivos,

62 YASSINE, Hadi M.; SHAH, Zubair. "How could artificial intelligence aid in the fight against coronavirus?". *Expert review of anti-infective therapy,* v.10, n.6, 2020, p.493-497. Disponível em: https://doi.org/10.1080/14787210.2020.1744275.
63 6 things about OpenTrace, the open-source code published by the TraceTogether team, GovTech Singapore, 09 set. 2020. Disponível em: https://www.tech.gov.sg/media/technews/six-things-about-opentrace.
64 Bloomberg. Israeli Spyware Firm Wants to Track Data to Stop Coronavirus Spreading, 2020. Disponível em: https://www.bloomberg.com/news/articles/2020-03-17/surveillance-company-nso-supplying-data-analysis-to-stop-virus. Acesso em: 12 set. 2020.

seja por não terem essa visão, seja por conta de que ações individuais sempre repercutem em consequências sociais mais amplas. No debate de "privacidade *versus* saúde em dimensão social" (ou saúde X segurança), ao natural, não prevalecerá um enquadramento individualista mesmo quando envolvendo a dignidade humana. Entretanto, o que se precisa é de determinação coletiva sobre as infraestruturas e instituições que processam os dados e que determinam como eles serão usados. Isso requer ir além da privacidade, implicando na escolha de optar ou não, por infraestruturas de vigilância de coronavírus público-privadas, assim como, quanto ao desenvolvimento de mecanismos democráticos para moldar a estrutura, aplicativos e agendas de arquiteturas tecnológicas ou *privacy by design*.

Em segundo lugar, mostram-se necessários mecanismos legais eficazes para garantir que o público tenha controle democrático sobre as novas infraestruturas tecnológicas. Atualmente, os dados gerados por nossos smartphones são absorvidos por provedores de sistemas operacionais, empresas de telecomunicações e desenvolvedores de aplicativos, mas a regulamentação e as responsabilidade são limitadas. Contudo, há espaço nesse ecossistema para outro grupo de atores que atuam no interesse das comunidades. Propostas como cooperativas de dados e fundos fiduciários podem facilitar a negociação coletiva entre usuários e grandes empresas de tecnologia e assim serem criados mecanismos para que essas coletividades usem e administrem dados democraticamente.

Em vez de aceitar a escolha na dicotomia excludente que envolve "privacidade" ou "saúde", será possível reestruturar o conjunto de escolhas e compensações em oferta. Para evitar a transferência de recursos de vigilância expandidos para empresas e estados, qualquer tentativa de utilizar dados para a mitigação do coronavírus poderia ser governada por fundos de dados ou outros mecanismos fiscalizatórios como Agência Nacional de Proteção de Dados (ANPD), caso a Autoridade Nacional de Dados criada pela LGPD não venha se mostrar eficiente e suficiente.

Terceiro e último, é primordial garantir que quaisquer sistemas/apps desenvolvidos sejam incapazes de se tornar formas arraigadas de vigilância e exploração de dados. As reformas de privacidade muitas vezes se concentram em atenuar os piores danos da vigilância, invocando a linguagem do direito internacional dos direitos humanos para exigir aplicações "necessárias, adequadas e proporcionais".

Nesse contexto, considerada a crise, tem-se que a confiança pública é a chave para garantir que todos se unam. A erosão da privacidade de dados pessoais, seria equivocada e prejudicial, tanto durante, quanto após esse momento aflitivo. Nesta luta colaborativa contra a COVID-19, todos temos a responsabilidade de agir, aconselhar e proteger: governos, empresas, ONGs e indivíduos. Esperamos que os insights aqui compartilhados possam em alguma maneira contribuir para a reflexão sobre as formas de encontrar e implementar uma adequada resposta comum neste momento de crise, pois tais medidas protegem, ao fim e ao cabo, todas as sociedades que jamais se desconectarão.

REFERÊNCIAS

6 things about OpenTrace, the open-source code published by the TraceTogether team, *GovTech Singapore,* 09 set. 2020. Disponível em: https://www.tech.gov.sg/media/technews/six-things-about-opentrace.

Tunisie Numerique*. A first in Tunisia: Pguard, the security robot to report violations,* 2020. Disponível em: <https://news-tunisia.tunisienumerique.com/tunisia-a-first-in-tunisia-pguard-the-security-robot-that-reports-violations/> Acesso em 07 set. 2020.

ALEUY, O. Alejandro; PITESKY, Maurice; GALLARDO, Rodrigo "Using multinomial and space-time permutation models to understand the epidemiology of infectious bronchitis in California between 2008 and 2012". *Avian diseases*, v. 62, n. 2, 2018, p.226-232. Disponível em: https://doi.org/10.1637/11788-122217-Reg.1.

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, p.67-79, 1999.

ALIMADADI, Ahmad; ARYAL, Sachin; MANANDHAR, Ishan; MUNROE, Patricia B.; JOE, Bina; CHENG, Xi. "Artificial intelligence and machine learning to fight Covid-19". *Physiological genomics*, v. 52, n. 4, 2020, p.200-202. Disponível em: https://doi.org/10.1152/physiolgenomics.00029.2020

ALLAM, Zaheer; JONES, David S. (2020). "On the coronavirus (Covid-19) outbreak and the smart city network: Universal data sharing standards coupled with artificial intelligence (AI) to benefit urban health monitoring and management". *Healthcare* (Basel, Switzerland), v. 8, n. 1. Disponível em: https://doi.org/10.3390/healthcare8010046.

Asociación para el Progreso de las Comunicaciones. *Ecuador: Las tecnologías de vigilancia en contexto de pandemia no deben poner en riesgo los derechos humanos,* 2020. Disponível em:https://www.apc.org/es/pubs/ecuador-las-tecnologias-de-vigilancia-en-contexto-de-pandemia-no-deben-poner-en-riesgo-los. Acesso em: 12. set. 2020.

AYYOUBZADEH, Seyed-Mohammad; AYYOUBZADEH, Seyed-Mehdi; ZAHEDI, Hoda; AHMADI, Mahnaz; KALHORI, Sharareh R. Niakan. "Predicting Covid-19 incidence through analysis of Google trends data in Iran: Data mining and deep learning pilot study". *JMIR Public health and surveillance*, v. 6, n. 2, 2020, e18828. Disponível em: https://doi.org/10.2196/18828.

BASTIAT, Frédéric. *A lei.* LVM Editora. Edição do Kindle, posição 222, 2019.

Bangalore Mirror. *Government publishes details of 19,240 home-quarantined people to keep a check,* 2020. Disponível em: https://bangaloremirror.indiatimes.com/bangalore/others/government-publishes-details-of-19240-home-quarantined-people-to-keep-a-check/articleshow/74807807.cms. Acesso em: 12. set. 2020.

BASTOS, Celso Ribeiro. *Curso de direito constitucional.* 21. ed. São Paulo: Saraiva, 2000.

BELTRÃO, Silvio Romero. *Direitos da personalidade:* de acordo com o Novo Código Civil. São Paulo: Atlas, 2005.

BENGTSSON, Linus; GAUDART, Jean; LU, Xin; MOORE, Sandra; WETTER, Erik; SALLAH, Kankoe; REBAUDET, Stanislas; PIARROUX, Renaud. "Using mobile phone data to predict the spatial spread of cholera". *Scientific reports*, v. 5, n. 1, 2015. Disponível em: https://doi.org/10.1038/srep08923.

BIONI, Bruno Ricardo. *Proteção de dados pessoais:* a função e os limites do consentimento. 2. ed. Rio de Janeiro: Grupo Editorial Nacional, 2020.

BIONI, Bruno. Compreendendo o conceito de anonimização e dado anonimizado. *Cadernos Jurídicos,* São Paulo, ano 21, nº 53, p. 191-201, jan./mar. 2020. Disponível em: https://api.tjsp.jus.br/Handlers/Handler/FileFetch.ashx?codigo=118902.

BITTAR, Carlos Alberto. *Os direitos da personalidade.* 7.ed. Rio de Janeiro: Forense Universitária, 2004.
Bloomberg. *Israeli Spyware Firm Wants to Track Data to Stop Coronavirus Spreading*, 2020. Disponível em: <https://www.bloomberg.com/news/articles/2020-03-17/surveillance-company-nso-supplying-data-analysis-to-stop-virus> Acesso em 07 set. 2020.

BRANDEIS, L. D.; WARREN S. D. The right to privacy. *Harvard Law Review*, Boston, v. 4, nº 5, dec., 1890.
Business Insider SA. *South Africa will be Tracking Cellphones to Fight the Covid-19 Virus*. 2020. Disponível em: <https://www.businessinsider.co.za/south-africa-will-be-tracking-cellphones-to-fight-covid-19-2020-3> Acesso em 07 set. 2020.

CARDOSO, Bruno. *Tecnopolíticas da vigilância.* Boitempo Editorial. Edição do Kindle. Posição 264. 2018.

CIS-India. Ebola: *A big data disaster,* 2016. Disponível em: https://cis-india.org/papers/ebola-a-big-data-disaster. Acesso em: 12 set. 2020.

CORDEIRO, A. Barreto Menezes. *Direito da Protecção de Dados* - À luz do RGPD e da Lei n.º 58/2019. Coimbra: Almedina, 2020.

CUPIS, Adriano de. *Os direitos da personalidade*. Trad. Afonso Celso Furtado Rezende. Campinas: Romana, 2004.

Dicionário Brasileiro da Língua Portuguesa. São Paulo: Encyclopaedia Brittannica do Brasil, 1987. v. 3.

DIEB, Daniel; GOMES, Helton Simões. Governo vai monitorar celular para controlar aglomeração na pandemia. [S.l.]: *UOL*, 2 abr. 2020. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2020/04/02/para-combater-a-covid-19-o-governo-federal-vai-monitorar-o-seu-celular.htm. Acesso em: 7 set. 2020.
Doc Sears. Do we have to "trade off"privacy?, *Doc Sears,* set. 2010.

DONEDA D.; ALMEIDA, B.A.; BARRETO, M.L. Uso e proteção de dados pessoais na pesquisa científica. *Revista Direito Público,* v.16, n.90, 2019, p.179-194.

DONEDA, D. *Da privacidade à proteção de dados pessoais.* São Paulo: Revista dos Tribunais, 2019.

European Data Protection Board. *Processing of personal data in the context of the COVID-19 outbreak,* 2020. Disponível em: https://edpb.europa.eu/news/news/2020/statement-edpb-chair-processing-personal-data-context-covid-19-outbreak_en. Acesso em: 12. set. 2020.

FERREIRA FILHO, M. G. *Curso de direito constitucional.* 33.ed. rev. e atual. São Paulo: Saraiva, 2007.

FERRETTI, L. *et al.* Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing. *Science,* v.368, n. 641, 08 maio 2020.

FRANÇA, Rubens Limongi. *Manual de Direito Civil.* 2. ed. São Paulo: Revista dos Tribunais, 1971, v. 1, p.321 *apud* FACHIN, Antonio Zulmar. *A proteção jurídica da imagem.* São Paulo: Celso Bastos, 1999.

Governo do Estado de São Paulo. *Governo de SP apresenta Sistema de Monitoramento Inteligente contra coronavírus.* 9 abr. 2020. Disponível em: https://www.saopaulo.sp.gov.br/noticias-coronavirus/governo-de-sp-apresenta-sistema-de-monitoramento-inteligente-contra-coronavirus. Acesso em: 12 set. 2020.

GUANAES P.; SOUZA A.R.; DONEDA D.; NASCIMENTO, F.J.T. *Marcos legais nacionais em face da abertura de dados para pesquisa em saúde:* Dados pessoais, sensíveis ou sigilosos e propriedade intelectual. Rio de Janeiro: Fiocruz; 2018.

HARARI, Yuval Noah. *The world after coronavirus.* Disponível em: https://www.ft.com/content/19d90308-6858-11ea-a3c9-1fe6fedcca75. Acesso em: 27 ago. 2020.

IN LOCO. *Política de Privacidade:* In Loco x COVID-19. 27 mar. 2020. Disponível em: https://www.inloco.com.br/pt/privacy-covid-19. Acesso em: 12. set. 2020.

La Hora. Sandoval sobre Alerta Guate: "Quien la quiera descargar lo puede hacer", 2020. Disponível em: < https://lahora.gt/sandoval-sobre-alerta-guate-quien-la-quiera-descargar-lo-puede-hacer/> Acesso em 07 set. 2020.

LAI, P. C.; WONG, C. M.; HEDLEY, A. J.; LEUNG, G. M. "Spatial clustering of SARS in Hong Kong". *Hong Kong medical journal* = Xianggang Yi Xue Za Zhi, v. 15, Suppl 9, 2009, p.17-19.

LANDAU, Susan. *Location Surveillance to Counter COVID-19:* Efficacy Is What Matters. 25 mar. 2020. Disponível em: <https://www.lawfareblog.com/location-surveillance-counter-covid-19-efficacy-what-

matters> Acesso em: 7 set. 2020.

Le Soir. *Coronavirus:* le cabinet De Block dit «oui» à l'utilisation des données télécoms , 2020. Disponível em: https://plus.lesoir.be/286535/article/2020-03-12/coronavirus-le-cabinet-de-block-dit-oui-lutilisation-des donnees-telecoms. Acesso em 12. set. 2020.

Lei n.13.979/2020. Dispõe sobre as medidas para enfrentamento da emergência de saúde pública de importância internacional decorrente do coronavírus responsável pelo surto de 2019. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/L13979.htm>. Acesso em: 17 set. 2020.

MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. *LGPD: Lei geral de proteção de dados comentada.* São Paulo: Thomson Reuters Brasil, 2019.

MCDONALD, Sean Martin. *Ebola:* A Big Data Disaster - Privacy, Property, and the Law of Disaster Experimentation. CIS Papers, 2016.

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

MORLEY, Jessica *et al.* Ethical guidelines for COVID-19 tracing apps. Nature, [s.l.], v. 582, n.7810, p.29-31, 28 maio 2020. *Springer Science and Business Media LLC.* Disponível em: http://dx.doi.org/10.1038/d41586-020-01578-0. Acesso em 7 set. 2020.

Organisation for Economic Co-operation and Development (Org.). *New mobile applications for COVID-19 "tracking" are also being launched.* 2020. Disponível em: http://www.oecd.org/coronavirus/policy-responses/tracking-and-tracing-covid-protecting-privacy-and-data-while-using-apps-and-biometrics 8f394636/#section-d1e108. Acesso em: 08 set. 2020.

Perú. *Debilidades de plataforma del Ministerio de Salud exponen información de pacientes COVID-19,* 2020. Disponível em: https://saludconlupa.com/noticias/peru-debilidades-de-plataforma-del-ministerio-de-salud-pueden-exponer-informacion-clinica-de-pacientes-covid-19/. Acesso em: 12 set. 2020.

Politico. *Commission tells carriers to hand over mobile data in coronavirus fight*, 2020. Disponível em: https://www.politico.eu/article/european-commission-mobile-phone-data-thierry-breton-coronavirus covid19/. Acesso em: 12 set. 2020.

Prefeitura da Cidade de Recife. *Prefeitura do Recife usa tecnologia como aliada na contenção do novo coronavírus.* 24 mar. 2020. Disponível em: http://www2.recife.pe.gov.br/noticias/24/03/2020/prefeitura-do-recife-usa-tecnologia-como-aliada-na-contencao-do-novo-coronavirus. Acesso em: 12 set. 2020.

RODOTÁ, S. *A vida na sociedade da vigilância* - a privacidade hoje. Rio de Janeiro: Renovar; 2008.

SANTOS, Boaventura de Sousa. *A cruel pedagogia do vírus* (Pandemia Capital) (p.4, posição 14). Boitempo Editorial. Edição do Kindle. 2020.

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

SILVA, J. A. *Curso de direito constitucional positivo.* 29. ed. São Paulo: Malheiros, 2007.

Supremo Tribunal Federal. MC - ADI 6387/DF, Rel. Min. Rosa Weber. CFOAB x Presidente da República. Disponível em: <http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADI6387MC.pdf>. Acesso em: 21 maio 2020.

STRAPAZZON, Carlos Luiz; INOMATA, Adriana. Restrições, Privações e Violações de Direitos Constitucionais Fundamentais. *Revista Eletrônica de Direito do Centro Universitário Newton Paiva*, Belo Horizonte, n.32, p.85-104, maio/ago., 2017, p.100. Disponível em: https://revistas.newtonpaiva.br/redcunp/wp-content/uploads/2020/05/N.32-06.pdf. Acesso em: 13 dez. 2020.

SZANIAWSKI, Elimar. *Direitos da personalidade e sua tutela.* 2.ed. São Paulo: Revista dos Tribunais, 2005.

TEPEDINO, Gustavo. *Temas de Direito Civil.* 3. ed. Rio de Janeiro: Renovar, 2004.

The New York Times. *In Coronavirus Fight, China Gives Citizens a Color Code, With Red Flags*, 2020. Disponível em: https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html. Acesso em: 12 set. 2020.

The Verge. *New study aims to use health data from a smart ring to identify coronavirus symptoms,* 2020. Disponível em: https://www.theverge.com/2020/3/23/21191225/coronavirus-smart-ring-oura-ucsf-san-francisco-general-hospital-tempredict. Acesso em: 12 set. 2020.

YASSINE, Hadi M.; SHAH, Zubair. "How could artificial intelligence aid in the fight against coronavirus?". *Expert review of anti-infective therapy*, v.10, n.6, p.493-497, 2020. Disponível em: https://doi.org/10.1080/14787210.2020.1744275.

Recebido em: 13.10.2020

Aprovado em: 10.12.2020

Como citar este artigo (ABNT):

PRUX, Oscar Ivan; PIAI, Kevin Henrique de Sousa. (Des)liberdade viral na pandemia: uma releitura da escalada por dados pessoais e seus impactos à luz dos direitos da personalidade e a proteção de dados. *Revista Eletrônica de Direito do Centro Universitário Newton Paiva*, Belo Horizonte, n.43, p.273-292, jan./abr. 2021. Disponível em: <https://revistas.newtonpaiva.br/redcunp/wp-content/uploads/2021/06/DIR43-16.pdf>. Acesso em: dia mês. ano.