REVISTA
CADERNO
VIRTUAL

VIGILÂNCIA MOVIDA A DADOS COMO MECANISMO DE COMBATE À COVID-19 E SEUS LIMITES ÉTICOS ENVOLTOS NA PROTEÇÃO DE DADOS PESSOAIS

Gabrielle Graça de Farias

Sumário

Resumo

O presente artigo aborda iniciativas tecnológicas movidas a dados pessoais como mecanismo de combate ao alastramento da pandemia da COVID-19. São analisados os casos de Singapura e Índia em relação à execução das iniciativas executadas em suas populações por meio de revisão bibliográfica de textos acadêmicos e notícias. Também são indicadas quais as situações dos países em relação aos direitos relativos à proteção de dados pessoais em seus respectivos cenários. Um panorama geral é traçado por meio da apresentação das condutas atuais em relação ao embate do direito à saúde e o direito à privacidade. Para demonstrar a falsidade da dicotomia, são apresentadas aplicações as quais protegem ambos os direitos. Para essa finalidade, são apresentados os parâmetros éticos os quais devem estar presentes nos empreendimentos movidos a dados. O artigo conclui que a adoção do sistema aplicado em Singapura é o mais efetivo na proteção dos direitos relativos à privacidade pela aplicação dos preceitos éticos adotados internacionalmente, quando comparado com a iniciativa de vigilância do contexto indiano. Aplicações envolvendo *contact tracing* aliadas ao modelo de concepção *privacy by design*, que segue os princípios adequados no tratamento de dados, desconstroem a falsa dualidade entre a saúde e privacidade.

Palavras-chave: Proteção de dados pessoais; Coronavírus; *Contact tracing*;

INTRODUÇÃO

O presente artigo se propõe a analisar alguns dos efeitos da pandemia do coronavírus no âmbito da vigilância digital, além das delimitações éticas necessárias para um tratamento de dados eficiente e legítimo. Primeiramente, são analisados os cenários de Singapura e Índia em relação às iniciativas de tecnologias movidas a dados e como elas funcionam no combate ao coronavírus.

Após o detalhamento de cada uma das iniciativas, um breve panorama sobre a situação de proteção dos dados pessoais envolvida nas situações é realizado, de acordo com a legislação e arquitetura das aplicações desenvolvidas. A partir dessas análises, é possível a identificação da situação da proteção desse direito em cada país no que tange as atividades de monitoramento.

A partir desse cenário é analisado como elementos presentes nesses dois ambientes, assim como o resto do mundo, têm sua origem no estado de calamidade gerado pela pandemia. Essas condições aliadas ao desenvolvimento tecnológico e científico promovem uma espécie de experimentalismo dos modelos de vigilância, aplicados no contexto de crise, em que mudanças drásticas são implementadas em um curto período de tempo, pouco se ponderando pelas consequências dessas ações. As novas iniciativas marcam a transição do modelo de vigilância exógena para a endógena, num regime elaborado por Yuval Harari[1].

Diante da necessidade e emergência da adoção de medidas para combater o alastramento da doença, junto ao fator de desenvolvimento tecnológico, surge o embate entre a proteção de dados e o direito a proteção da saúde. O dilema induz uma falsa dicotomia uma vez que ambos os direitos devem estra aliados nas iniciativas propostas, não elaboradas como polos opostos. É possível a construção de meios os quais sejam epidemiologicamente efetivos, assim como estejam em alinhamento com os princípios éticos essenciais da proteção das informações de seus titulares.

Duas possibilidades de aplicações que fazem uso da tecnologia de *contact tracing* são apresentadas: por meio de pontos de *checkpoints* e do sinal de *bluetooth*. A primeira é uma iniciativa que demanda maior atenção e engajamento dos usuários; a segunda possui maior possibilidade de adesão pela sua construção. Ambas as aplicações são desenvolvidas com a privacidade em foco na sua idealização, construção e execução, respeitando os limites da privacidade, exercendo a coleta mínima de informações e anonimizando na medida do possível os dados coletados e, se for o caso, compartilhados.

No desenvolvimento dessas iniciativas ilustradas, assim como quaisquer outras que envolvam dados pessoais - sejam sensíveis ou não - devem seguir determinados parâmetros de limitação em sua utilização. Princípios relacionados à privacidade estipulados na Convenção Europeia de Direitos Humanos, do Pacto Internacional dos Direitos Civis e Políticos (PIDCP)

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

e dos Princípios de Siracusa das Nações Unidas são limitadores no que tange ao tratamento ético de dados.

1 VIGILÂNCIA MOVIDA A DADOS NO COMBATE AO CORONAVÍRUS

1.1 Contexto mundial diante da pandemia

Com aproximadamente dezessete milhões de infectados e mais de quatrocentas mil mortes no mundo inteiro[2], a Síndrome Respiratória Aguda associada ao Coronavírus (SARS-CoV-19), ou, simplesmente COVID-19, continua fazendo vítimas em todo o mundo. Os primeiros registros do vírus foram na China, ao final do ano de 2019. Poucos meses depois, em março de 2020, a Organização Mundial de Saúde declarou o *status* de pandemia global causada pela doença[3].

A proporção do problema exigiu medidas preventivas e de combate que mudaram os hábitos da população mundial. A aplicação de medidas de *lockdown* foram impostas em todo mundo, com o objetivo de achatar o crescimento da curva de contágio para que os sistemas de saúde comportem os pacientes que necessitem de internação. A testagem da população em massa também foi uma das medidas implementadas para que fosse possível o controle e registro dos casos efetivos nos países.

Diversos fatores fizeram com que a situação chegasse a esse ponto. A velocidade da transmissão viral é alta, além de haver pessoas que adquirem o vírus e não manifestam sintomas, repassando-os sem saber[4]. Ademais, em casos sintomáticos, a fase de transmissão viral ocorre antes de que o infectado manifeste indícios de que está contaminado, tornando difícil o rastreamento e a adoção de medidas que impeçam a infecção em terceiros.

Outro fator essencial na ampliada escala de disseminação é a globalização aliada à revolução digital e tecnológica que atingimos no último século[5]. O alto fluxo de pessoas garantiu o espalhamento da doença por diversos centros urbanos. Cidades densas e com maiores

---

[2] WORLD HEALTH ORGANIZATION. **WHO Coronavirus Disease (COVID-19) Dashboard**. Disponível em: https://covid19.who.int/. Acesso em: 30 jun. 2020.

[3] BBC. **Coronavírus: OMS declara pandemia**. 2020. Disponível em: https://www.bbc.com/portuguese/geral-51842518. Acesso em: 01 abr. 2020.

[4] G1. **OMS esclarece que assintomáticos transmitem coronavírus: 'a questão é saber quanto'**. 2020. Disponível em: https://g1.globo.com/bemestar/coronavirus/noticia/2020/06/09/transmissao-por-casos-assintomaticos-esta-ocorrendo-a-questao-e-saber-quanto-diz-oms.ghtml. Acesso em: 09 jun. 2020.

[5] KEESARA, Sirina *et al*. **Covid-19 and Health Care's Digital Revolution**. Disponível em: https://www.nejm.org/doi/full/10.1056/NEJMp2005835. Acesso em: 22 maio 2020. p. 1.

índices de urbanização apresentam maior concentração de casos, como no caso da cidade de São Paulo[6].

Se a evolução digital foi um dos fatores determinantes para a instauração da maior crise de saúde pública dos últimos 100 anos, nela também estão as soluções. O uso de plataformas de monitoramento e vigilância movidos a dados têm sido utilizadas como meio de combate ao coronavírus. Uso de tecnologias com base em reconhecimento facial, instalação de termômetros em aeroportos, aplicativos que rastreiam por onde infectados andaram: inúmeras são as aplicações da vigilância digital no enfrentamento à pandemia. Analisemos os casos de alguns países que fazem uso dessas tecnologias.

1.1.1 Singapura

Em Singapura, o aplicativo *TraceTogether* é utilizado pelo governo como um dos pilares da vigilância tecnológica no auxílio do controle à pandemia, estruturado com base na coleta de dados por meio da tecnologia *bluetooth*. A coleta é referente a informações como proximidade e a duração do tempo do contato de um usuário com o outro. Se algum deles for testado como positivo, é solicitado que ele compartilhe os dados com o Ministério da Saúde de Singapura para que haja a notificação de todos os usuários que tiveram contato por determinado tempo e distância com o contaminado[7].

Os dados coletados são referentes à identificação pessoal do usuário – nome e número de celular – e suas interações com outros usuários, informações referentes ao aplicativo, assim como os dados de processamento pelo próprio celular[8]. Não há a coleta de dados por meio de geolocalização e o processamento e registro desses são realizados internamente no aparelho celular. Há apenas o compartilhamento com terceiros se o usuário for testado como positivo para a doença[9]. De acordo com o site do app, não há a coleta para fins indevidos[10], além de haver a possibilidade da retirada do nome do cadastro. Há o compartilhamento dos dados com

---

[6] ESTADÃO. **Pelo terceiro dia seguido, SP tem mais de 5.500 novos casos de covid-19; mortes vão a 7.532**. 2020. Disponível em: https://saude.estadao.com.br/noticias/geral,pelo-terceiro-dia-seguido-sp-tem-mais-de-5500-novos-casos-de-covid-19-mortes-vao-a-7532,70003319919. Acesso em: 30 maio 2020.

[7] FORBES. **Conheça o TraceTogether, app de monitoramento do coronavírus criado por Singapura**. 2020. Disponível em: https://forbes.com.br/negocios/2020/03/conheca-o-tracetogether-app-de-monitoramento-do-coronavirus-criado-por-singapura/. Acesso em: 27 maio 2020.

[8] TRACETOGETHER. **What data is collected? Are you able to see my personal data?** 2020. Disponível em: https://support.tracetogether.gov.sg/hc/en-sg/articles/360043735693-What-data-is-collected-Are-you-able-to-see-my-personal-data-. Acesso em: 08 jun. 2020.

[9] *Idem*. **How is my data protected?** 2020. Disponível em: https://support.tracetogether.gov.sg/hc/en-sg/articles/360043234694-How-is-my-data-protected-. Acesso em: 08 jun. 2020.

[10] *Idem*. **TraceTogether Privacy Safeguards**. Disponível em: https://www.tracetogether.gov.sg/common/privacystatement. Acesso em: 08 jun. 2020.

hospitais locais, além do Ministério da Saúde local e terceiros[11], mas o governo assume o compromisso de que compartilhamento com terceiros sejam apenas de dados anonimizados, sendo impossível, segundo eles, que haja a reindentificação do usuário.

Há pontos passíveis de crítica no que tange a proteção de dados pessoais. Por mais que haja a garantia de que as informações sejam anonimizadas antes de serem compartilhadas com terceiros – técnica denominada de *release-and-forget* - há indícios de que, a partir de determinado modelo, é possível a "desanonimização" com a acurácia de 99,98% de acerto nos dados[12]. No estudo, foi utilizada uma base de dados com informações incompletas acerca de pessoas naturais e, como resultado final, foi possível a reidentificação com base em quinze atributos demográficos.

Comparando com o contexto do *TraceTogether*, os dados coletados para o funcionamento do aplicativo dentro dos parâmetros de privacidade estabelecido pelos desenvolvedores podem não ser suficientes para a identificação dos usuários. No entanto, se os terceiros que obtiverem acesso a essas informações tiverem acesso a outra base de dados com base em *Big Data*, há pontos suficientes para que os dados das duas bases sejam cruzados, relevando novas informações obtidas a partir do tratamento.

Além dessas vulnerabilidades, a captura dos dados não é completamente anonimizada pois o número de identificação do *bluetooth* é atrelado ao número de celular do dono do aparelho, tornando possível a identificação pela central dos dados acerca de quem foi diagnosticado com a COVID-19 e com quem a pessoa teve contato. Conforme será demonstrado adiante, o monitoramento com foco epidemiológico é perfeitamente possível de ser realizado sem a necessidade da vinculação com qualquer dado pessoal e de forma descentralizada, respeitando a mínima coleta de dados e mínima intervenção, reduzindo as possibilidades de reidentificação das pessoas naturais as quais as informações pertencem.

1.1.2 Índia

Yuvah Noah Harari, em sua análise do cenário atual em relação às mudanças promovidas pelo coronavírus, descreve um exemplo hipotético[13]: um governo determina que

[11] OECD. **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 jun. 2020.
[12] ROCHER, Luc. **Estimating the success of re-identifications in incomplete datasets using generative models**. Disponível em: https://www.nature.com/articles/s41467-019-10933-3. Acesso em: 08 jun. 2020. p.1.
[13] *Ibidem.*

os habitantes de seu país devem utilizar um bracelete que monitora a temperatura corporal, localização, seus batimentos cardíacos, entre outros sinais. Com o processamento das informações, seria possível determinar se a pessoa está doente, com quem ela teve contato e sua fonte de contração da doença, entre outras informações, consistindo em um meio extremamente eficaz no acompanhamento da doença. No entanto, o custo de um alto nível de monitoramento é o esgotamento da privacidade e limitação no poder de escolha das pessoas[14].

A situação trazida pelo autor não é mais hipotética. O governo indiano anunciou uma iniciativa de fabricar braceletes digitais que monitoram diversas informações sobre o *status* de saúde do usuário[15]. Os aparelhos serão utilizados junto com o aplicativo "*Aarogya Setu"*, que determina o risco de infecção aos usuários, destinado à população em geral. O dispositivo será utilizado no monitoramento de trabalhadores de serviços essenciais, assim como pacientes que estiverem infectados com o vírus ou sob suspeita. Caso alguma pessoa infectada saia do perímetro virtual determinado pelo aplicativo, será emitido um sinal de forma automática às autoridades locais para intervenção. Com as informações coletadas é possível determinar como o local que a pessoa infectada visitou, os caminhos utilizados por ela, se houve qualquer tipo de pessoa doente está por perto[16].

A empresa Broadcast Engineering Consultant India Limited (BECIL), responsável pela elaboração das *wristbands*, descreve a iniciativa como "uma plataforma de inteligência investigativa e um mecanismo tático de prevenção e investigação de ameaças à segurança nacional[17]". A abrangência da iniciativa e a ausência de mecanismos de transparência que definam os critérios de funcionamento do app preocupa. 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

---

[14] *Ibidem.* "A desvantagem é, obviamente, que isso daria legitimidade a um novo e aterrador sistema de vigilância. Se você sabe, por exemplo, que cliquei no link da Fox News em vez do link da CNN, isso pode lhe ensinar algo sobre minhas opiniões políticas e talvez até sobre minha personalidade. Mas se você puder monitorar o que acontece com a temperatura do meu corpo, a pressão sanguínea e o batimento cardíaco enquanto assisto ao videoclipe, você pode aprender o que me faz rir, o que me faz chorar e o que me deixa muito, muito zangado. (...) Se as empresas e os governos começarem a coletar nossos dados biométricos em massa, eles podem nos conhecer muito melhor do que nós mesmos, e podem não apenas prever nossos sentimentos, mas também manipular nossos sentimentos e vender-nos o que quiserem - seja um produto ou um político." Tradução nossa.

[15] INDIA, The Times Of. **India plans wristband patient surveillance as lockdown eases**. 2020. Disponível em: https://timesofindia.indiatimes.com/india/india-plans-wristband-patient-surveillance-as-lockdown-eases/articleshow/75300967.cms. Acesso em: 12 maio 2020.

[16] INDIA, loc. cit.

[17] WEB, The Next. **India wants to build an ultra-intrusive 'wristband' to track coronavirus patients' every move**. 2020. Disponível em: https://thenextweb.com/in/2020/04/22/india-wants-to-build-an-ultra-intrusive-wristband-to-track-coronavirus-patients-every-move/. Acesso em: 13 maio 2020.

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[18].

Não há um regramento específico nacional que delimite os parâmetros para o uso e coleta responsável dos dados no contexto indiano. No entanto, os princípios do Código de Práticas Justas de Informação – *Code of Fair Information Practices* –, proposto pelo Departamento de Saúde, Educação e Bem-Estar dos Estados Unidos da América (EUA) em 1973[19] define um conjunto de boas práticas, que, apesar de ser originado no contexto norte-americano, podem servir como um guia de princípios no desenvolvimento e execução do programa.

O aplicativo deveria ser construído num molde *privacy by design*, com base nas seguintes orientações: (*i*.) a existência de nenhum sistema de coleta de dados pessoais pode ser secreto; (*ii*.) deve ser garantido aos indivíduos meios de saber quais informações sobre ele estão armazenadas e como são utilizadas; (*iii*.) deve haver mecanismos de prevenção ao desvio de finalidade dos dados coletados, qualquer outro uso sem o consentimento para tal deve ser vedado; (*iv*.) meios de correção ou emenda das informações relativas ao usuário devem ser assegurados; (*v*.) qualquer organização que venha a manipular os dados pessoais identificáveis deve certificar que haja prevenção para evitar seu uso indevido, assim como garantir a confiabilidade dos dados para o uso pretendido.

Apesar de não haver um marco legal específico envolvendo o uso de dados na Índia, o direito à privacidade como uma garantia constitucional foi reconhecido pela Suprema Corte da Índia em 2017. O caso foi motivado pela formação de um banco de dados pelo governo indiano por meio do "*Aadhar Project*", que dados como informações biométricas, impressões da retina e informações demográficas eram associadas à dados como contas de banco, registros médicos e números de telefone[20]. A Corte, em uma decisão histórica, reconheceu que o direito à

---

[18] WEB, *loc. cit.*

[19] CENTER, Electronic Privacy Information. **The Code of Fair Information Practices**. 2020. Disponível em: https://epic.org/privacy/consumer/code_fair_info.html. Acesso em: 19 maio 2020. O conjunto de princípios foi originado para um uso adequado da informação com base na privacidade, *fairness* e segurança. Mais em: https://www.worldprivacyforum.org/2008/01/report-a-brief-introduction-to-fair-information-practices/.

[20] GURUSWAMY, Menaka. Justice K.S. Puttaswamy (Ret'd) and Anr v. Union of India and Ors. **American Journal Of International Law**, [s.l.], v. 111, n. 4, out. 2017. Cambridge University Press (CUP). http://dx.doi.org/10.1017/ajil.2017.92. Disponível em: https://www.cambridge.org/core/journals/american-journal-of-international-law/article/justice-ks-puttaswamy-retd-and-anr-v-union-of-india-and-ors/ED631B8F922039BEC5400086C8E34338. Acesso em: 15 jun. 2020. p. 1.

privacidade é uma derivação dos direitos à igualdade, à dignidade, à fala, à expressão, à vida e à liberdade.

Apesar das garantias constitucionais, o aplicativo foi moldado em completo desacordo com as orientações que preservam esses direitos. É essencial um marco regulatório que delimite a atuação da iniciativa indiana, considerando os preceitos de respeito à finalidade da coleta, transparência no tratamento dos dados, garantia da coleta mínima, controle do titular sobre o bloqueio e eliminação de seus dados, o direito à revisão automatizada e à supervisão humana, o direito à correção e atualização em seu respectivo banco de dados, à garantia de que as informações serão armazenadas em um ambiente seguro e que previna ataques e vazamentos[21], entre outras medidas.

1.1.3 Aspectos comuns

A crise do coronavírus e a pressa para tomada de decisões urgentes fazem com que tecnologias imaturas, como as retratadas acima, sejam implementadas sem maiores reflexões acerca de como elas impactam a vida em sociedade, ou a proteção de direitos relacionados em dados. A maneira a qual a pandemia se espalha pelo globo não permite que ações sejam testadas à exaustão ou que todas as suas hipóteses de interferência sejam devidamente amadurecidas. Fator esse que garante uma forte amplitude de mudança no cenário mundial com base nas decisões tomadas hoje pelos governantes[22]. O cenário atual é como um grande painel de experimentos sociais acerca de como a tecnologia moldará a vida em sociedade de acordo com seus parâmetros de funcionamento, em casos que esses forem existentes.

Toda essa estrutura traça dois marcos: a concretização da vigilância em massa e a transição de uma vigilância "exógena" (*over-the-skin surveillance*) para uma vigilância "endógena" (*under-the-skin surveillance*)[23]. O primeiro marco já estava em andamento com a implementação de diversos meios de extração de dados para conversão desses em informação e a respectiva capitalização. Em troca das informações são ofertados serviços como serviços de

[21] DEB, Sidharth. **Privacy prescriptions for technology interventions on Covid-19 in India**. 2020. Coordenada por Internet Freedom Foundation. Disponível em: https://drive.google.com/file/d/1UK5rElhcdP5T3Y-8fYP6cCgQKKpQBeOX/view. Acesso em: 25 maio 2020. p. 74-76.
[22] HARARI, *Op. cit.*
[23] *Ibdem.*

mapas online pelo *Google Maps*[24] ou aplicativos de mudança de aparência com base em inteligência artificial, como o *Face App*[25].

O critério pré-crise para a utilização de tecnologias era a comodidade de serviços inteligentes, entretenimento ou otimização de tarefas. Hoje, a parcela que é oferecida em troca dessas tecnologias de vigilância é o exercício de direitos fundamentais. Afinal, em um cenário como esse, quem não se submeteria a um aplicativo que rastrearia seus movimentos em detrimento de poder sair de casa numa tentativa de retomada de uma rotina sem restrições sociais por conta do COVID-19?

Nesse processo, há o segundo marco. A vigilância "exógena" é relativa ao monitoramento mais usual, em relação a dados de localização, tempo utilizado em uma determinada página na web ou pesquisas realizadas que envolvem certo produto a ser consumido. Esses mecanismos são utilizados em grande escala com finalidades diversas, a maioria delas relativas ao emprego de marketing direcionado.

Com a pandemia, dados relativos à saúde dos titulares se tornaram mais relevantes porque, por meio do controle deles, o rastreamento da doença pode ser realizado e a transmissão evitada. Há a justificativa perfeita para a implementação dessa nova forma de monitoramento. Caso não haja uma estrita regulação acerca da utilização de todas essas informações, a liberdade humana e a democracia estarão ameaçadas por algoritmo de predição comportamental.

2 O FALSO EMBATE ENTRE A PROTEÇÃO DE DADOS E O COMBATE AO CORONAVÍRUS

Com o pretexto da pandemia, é construído um dilema entre o direito à proteção de dados pessoais e o direito à saúde. De um lado, há a necessidade de aplicação de todos os meios necessários no combate à pandemia, em suas formas mais desenvolvidas e que possuam maiores impactos para impedir o espalhamento da doença. Por outro, há todo o risco envolvendo o abuso de direitos decorrentes da implementação desses tipos de mecanismos.

---

[24] EXPRESS. **Google Maps is tracking you! How your smartphone knows your every move: a mapping device on a popular brand of smartphone keeps a record of each journey you take**. 2014. Disponível em: https://www.express.co.uk/life-style/science-technology/500811/Google-Maps-is-tracking-your-every-move. Acesso em: 16 maio 2020.

[25] POST, The Washington. **You downloaded FaceApp. Here's what you've just done to your privacy.** 2019. Disponível em: https://www.washingtonpost.com/technology/2019/07/17/you-downloaded-faceapp-heres-what-youve-just-done-your-privacy/. Acesso em: 15 jun. 2020.

O cerne desse falso embate está justamente em sua criação. A intervenção em direitos e garantias fundamentais é justificada pelo COVID-19, justamente por ser considerada preferível a proteção à economia[26] – prejudicada por conta da pandemia - e o direito de ir e vir – limitado por conta das medidas restritivas e do *lockdown* -. Não deve haver a elaboração de um panorama em que esses dois direitos estejam em polos opostos: eles devem estar conjugados nas iniciativas desde o momento em sua concepção, num modelo *privacy-by-design*, que vise o empoderamento popular em detrimento de uma vigilância totalitária[27].

Os aplicativos de *contract tracing* têm a enorme potencialidade de aliar o combate à doença, respeitando a proteção aos dados pessoais dos titulares. Eles utilizam os aparelhos celulares como meio de informação aos usuários acerca de possíveis contatos com pessoas infectadas[28]. A partir desse contato, é seguido o protocolo local para testagem ou isolamento. Nessa construção, há a maior efetividade no controle da doença, em uma perspectiva epidemiológica, além de uma mínima coleta de dados e informações sobre os usuários[29]. Analisemos duas modalidades de *contact tracing*, a primeira baseada na geração de *checkpoints* e a segunda, por meio da tecnologia *bluetooth*.

2.1 *Contact tracing* por meio de *checkpoints* e *bluetooth*

O aplicativo funcionaria em uma plataforma em que os usuários podem criar diversos checkpoints de acordo com os lugares que eles frequentam. Cada um, por meio de seu aplicativo, digitaliza o código QR gerado para aquela determinada interação social, ficando ali registrado que determinado usuário esteve naquele ambiente em um determinado momento, seja em uma estação de metrô, um restaurante ou uma pequena reunião entre amigos. As pessoas que fossem diagnosticadas como infectadas iriam notificar a plataforma de forma voluntária, assim, o aplicativo poderia tratar as informações e gerar os gráficos de transmissão a partir dos lugares que a pessoa esteve. Dessa maneira, os usuários que estiveram nos

---

[26] ABELER, Johannes; BÄCKER, Matthias; BUERMEYER, Ulf; ZILLESSEN, Hannah. **COVID-19 Contact Tracing and Data Protection Can Go Together.** Jmir Mhealth And Uhealth, [s.l.], v. 8, n. 4, 20 abr. 2020. JMIR Publications Inc.. http://dx.doi.org/10.2196/19359. Disponível em: https://mhealth.jmir.org/2020/4/e19359/. Acesso em: 15 jun. 2020. p. 1.

[27] HARARI, *Op. cit.*

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

[29] ABELER, Johannes; BÄCKER, Matthias; BUERMEYER, Ulf; ZILLESSEN, Hannah. **COVID-19 Contact Tracing and Data Protection Can Go Together**. Jmir Mhealth And Uhealth, [s.l.], v. 8, n. 4, 20 abr. 2020. JMIR Publications Inc.. http://dx.doi.org/10.2196/19359. Disponível em: https://mhealth.jmir.org/2020/4/e19359/. Acesso em: 15 jun. 2020. p. 4.

checkpoints nos mesmos momentos em que os infectados estiveram estarão cientes da possibilidade de transmissão e do risco de estarem infectados[30].

Não há a necessidade de registro em um perfil para a utilização da plataforma, ou seja, não há a vinculação com dados dos usuários pois a notificação é feita a partir do número de identificação que os aparelhos possuem. No entanto, a arquitetura do aplicativo requer a vigilância constante de, ao adentrar em determinado espaço, fazer o escaneamento do código, além da vontade de participação por uma parte significante da população por um período de constante, não apenas no início da adoção do programa. Esses elementos podem vir a comprometer a eficácia do programa, uma vez que o fator de atenção pode vir a esvaziar toda a efetividade do aplicativo.

Um dos elementos essenciais para o bom funcionamento da tentativa é o acesso à tecnologia em termos da população em geral. De pouco adianta uma iniciativa a qual o grupo foco não venha a ser atingido, seja por um problema causado pela necessidade de vigilância constante dos usuários, seja pela falta de acesso à tecnologia.

Outra iniciativa é a de *contact tracing* por *bluetooth*, cuja a característica de emissão de frequências de baixa energia a torna uma boa opção. Vejamos: em um ambiente com diversas pessoas e se todas elas possuírem um aparelho celular que esteja com a rede sem fio ligada, cada um deles é capaz de detectar o sinal dos outros em um determinado raio de distância. Quando mais próximos os aparelhos, mais fortes os sinais estarão um do outro, maior será a interferência; quanto mais distantes, mais fracos, menor a interferência.

As interações ficam registradas em cada aparelho que cruzar a área de alcance do sinal, estando inclusos o tempo de duração, assim como a distância entre os usuários, que é identificável pela intensidade da intersecção dos sinais. Essas características pertencentes ao *bluetooth* são fatores que os tornam valiosos na perspectiva de combate à doença. Como a transmissão da COVID-19 geralmente é dada a partir do contato físico próximo entre duas pessoas, a partir de uma determinada distância e um determinado período de tempo, um mecanismo que é capaz de metrificar esses dois elementos se faz muito valioso no ponto de vista epidemiológico.

O aplicativo funciona da seguinte maneira: o programa geraria um número de identificação do aparelho de forma criptografada a cada trinta minutos e, quando duas pessoas

[30] Ibidem. p. 2.

que forem usuárias do app estiverem próximas umas da outras, seus aplicativos registrariam a identificação temporária uns dos outros. Assim, há a indicação de que elas estiveram em contato no momento em que aqueles números estavam identificando os aparelhos. Todo o histórico de informações acerca das interações é encriptado e armazenado localmente no celular dos usuários.

Quando ocorrer o diagnóstico por coronavírus por algum usuário, o médico responsável pelo paciente questionaria se haveria interesse do usuário compartilhar a lista de números de identificação presente em seu celular para uma central de dados. A central tem acesso às interações e notifica os usuários que tiveram aquele número gerado no momento do contato com o contaminado. Não há a necessidade de vínculo com nenhum dado pessoal pois a única informação necessária é a lista de números que tiveram contato entre si[31]. Os usuários que tivessem risco de serem infectados por conta do contato próximo com o doente são notificados para procurar as autoridades locais para a realização de testagem e a adoção do isolamento social.

Essa configuração de *contact tracing* não implementa o ônus da constante atenção ao adentrar em quaisquer locais com interação social que o sistema de *checkpoints* impõe, tornando mais fácil e provável a adoção e permanência de uso do aplicativo, uma vez que a única ação necessária é deixar o sinal constantemente ligado no aparelho celular.

Além do mais, é uma alternativa mais precisa e com menor intervenção na privacidade quando comparado ao sistema de geolocalização, uma vez que o sistema possui a precisão máxima de dois metros ao determinar a posição de uma pessoa[32]. A distância é muito superior ao necessário quando se leva em consideração analisar o contágio de uma doença que acontece por distâncias menores, e, a depender, do período de tempo de contato.

Contudo, há pontos negativos que devem ser levados em consideração na implementação de um sistema como esse. O primeiro é que a efetividade de um programa como esse só depende o empenho do poder público na realização de campanhas de testagem em massa, adoção de medidas de restrição social, obrigatoriedade do uso de máscaras. O aplicativo não é a solução para o combate ao coronavírus, mas uma medida auxiliar que amplifica de modo significativo a prevenção e acompanhamento da doença quando aplicado com essas outras medidas.

---

[31] Ibidem. p. 2-3.
[32] Ibidem. p. 2-3.

Outro ponto relativo ao app em si, é o acesso da população às tecnologias digitais, principalmente aparelhos celulares que disponham do sinal *bluetooth*. Para que haja eficácia no acompanhamento do desenvolvimento da pandemia é necessária a adesão de uma boa parcela da população ao programa. O aplicativo deve ser moldado em uma interface acessível e os objetivos do uso, bem explicados. Os usuários devem saber qual sua finalidade, importância, e como os seus direitos e dados estão sendo resguardados pela plataforma.

A confiança no governo e na ciência é um fator central no sucesso da implementação de um sistema como esse. A ausência de transparência, a descrença pública com o Estado e governo, além do negacionismo cientifico podem pôr em xeque toda a estrutura de combate ao coronavírus.

Um ponto técnico relativo à execução da aplicação que pode ativar falsos alarmes de contato é o fato de que o sinal não é separado por paredes, assim, podendo levar a uma série de falsos positivos. Quando consideramos por exemplo, um prédio habitacional com alta densidade de pessoas, elas podem não ter contato físico entre si pois estão em ambientes separados com obstáculos físicos, mas ainda estão próximas o suficiente de modo que estejam no raio do sinal de *bluetooth* uns dos outros[33]. Caso uma dessas pessoas seja testada como positivo para COVID-19, todos aqueles que estiverem nessa proximidade também serão alertados como potenciais infectados, ainda que não tivessem contato físico um com os outros. Esse tipo de erro pode ensejar desconfiança nos usuários por conta do número de falsos alarmes.

2.2 Princípios éticos nas iniciativas de *contact tracing*

As alternativas de *contact tracing* podem representar a perfeita contraposição a criação do cenário de oposição entre a proteção de dados pessoais e o direito à saúde, em relação às iniciativas de combate ao coronavírus. Para isso, é necessária a adoção de princípios éticos em uma elaboração centrada no *privacy by design*. A partir da derivação de princípios oriundos da Convenção Europeia de Direitos Humanos, do Pacto Internacional dos Direitos Civis e Políticos (PIDCP) e dos Princípios de Siracusa das Nações Unidas, é possível determinar quatro princípios éticos centrais: necessidade, proporcionalidade, validade científica e limitação no tempo[34].

[33] MORLEY. *Op. cit.* p. 30.
[34] MORLEY, *Op. Cit.* p. 31.

A necessidade está vinculada a presença de fatores que tornem as medidas imprescindíveis quando analisado o cenário como um todo. No combate a pandemia, ao se considerar o contexto de urgência causado pelas inúmeras mortes e infectados, paralisação de atividades essenciais e intensas restrições nos direitos de liberdade, o desenvolvimento de tecnologias nesse sentido conferem o aspecto da necessidade.

Dentro desse fator, surge um subprincípio da finalidade, afinal, os dados são coletados dentro de um escopo de um problema de saúde pública, logo, qualquer utilização de dados que fuja dessas limitações rompem com o princípio supracitado. Os dados devem ser coletados e armazenados apenas para esses fins, com absoluta restrição de uso para quaisquer outros fins, principalmente envolvendo o uso comercial desses[35].

A proporcionalidade do aplicativo também deve ser estritamente conectada ao uso mínimo de dados. Por mais que a pandemia não possua precedentes na história da humanidade, o contexto de excepcionalidade não exclui a necessidade de medidas restritivas ao uso dos dados da população monitorada. Assim, a coleta e processamento de dados devem manter a proporcionalidade, sendo devidamente justificada por interesses legítimos de envolvam a situação de saúde pública, além de serem estritamente adequado para atingir os objetivos declarados.

Programas como o *app* indiano *Aarogya Setu* vão em encontro direto com todas essas orientações, devido a sua amplitude de coleta de dados de forma desproporcional, afinal, a extração de dados como o que o titular solicita em aplicativos de comida é díspar com a finalidade de contenção da doença.

O preceito da coleta mínima de dados procede com a definição da proporcionalidade pois uma coleta proporcional é uma coleta mínima. Não há necessidade de um número maior de informações do que o fundamental para a finalidade do aplicativo. O *contact tracing* via *bluetooth*, apenas as informações referentes ao número de identificação dos celulares, que é gerado pelo próprio aplicativo, assim como a lista de interações que envolvam determinado espaço e período de tempo são os dados fundamentais para o funcionamento do programa. No contexto de Singapura com o *TraceTogether*, o número de telefone é vinculado ao aplicativo,

[35] World Health Organization (org.). **Ethical considerations to guide the use of digital proximity tracking technologies for COVID-19 contact tracing**. 2020. Disponível em: https://www.who.int/publications/i/item/WHO-2019-nCoV-Ethics_Contact_tracing_apps-2020.1. Acesso em: 21 jun. 2020. p. 3.

requisitando informações não essenciais[36], incidindo na violação do princípio da proporcionalidade.

Em relação à validade científica, todas as medidas adotadas devem possuir o devido respaldo e comprovação de que possuem eficácia no combate à pandemia. A adoção de um mecanismo tecnológico movido a dados deve ser baseado em posicionamentos devidamente estudados e testados pela comunidade científica. Por mais que a situação seja extraordinária, há devidos estudos no âmbito da virologia que apontam os fatores centrais da transmissão. Logo, as alternativas de *contact tracing* devem estar presas a esses fatores biológicos na elaboração do *software*. O aplicativo baseado em *bluetooth* leva em consideração os fatores de contágio pelo ar, e para isso, é necessária a proximidade entre duas pessoas. Logo, a maneira ética de desenvolvimento da aplicação deve ser pautada nesse elemento que caracteriza todo o ciclo de contágio.

Por último, o princípio da limitação ao tempo é essencial. As medidas de vigilância devem estar estritamente ligadas a duração da pandemia. Os governos e sistemas de saúde utilizarão de todos esses dados unicamente com o propósito de enfrentamento da crise do coronavírus. Não há motivos para que todo esse sistema seja perpetuado para tempos além dos necessários, sob o risco de consolidação de um sistema de vigilância que venha a ser desviado para outras finalidades diversas. Assim, a partir do momento em que for declarado o fim da pandemia, na grande escala em que atualmente se encontra, todos esses instrumentos de monitoramento devem ser desarticulados[37] e todos os dados armazenados devem ser retirados de seus diretórios para evitar quaisquer tipos de ilicitudes e desvios.

CONCLUSÃO

A humanidade jamais enfrentou os desafios na escala em que enfrenta nesse momento devido ao enorme desenvolvimento tecnológico atingido no último século. A crise mundial do COVID-19 é um efeito de toda essa dimensão. Se, graças à tecnologia, houve o espalhamento desse patógeno em escalas as quais não foram vistas em eventos anteriores, havemos também inúmeros instrumentos de combate ao coronavírus.

[36] ABELER. *Op. Cit.* p. 4.
[37] World Health Organization (org.). *Op. Cit.* p. 3.

Os elementos essenciais para o controle e metrificação da doença são a testagem em massa, a adoção de políticas de restrição social, e o uso de tecnologia para controlar o repasse do vírus. Em Singapura, adotou-se o aplicativo de *contact tracing* "*TraceTogether"* para mapear aonde pessoas infectadas passaram e com quem tiveram contato, para que quem houvesse tido aproximação com um contaminado por um determinado período de tempo fosse orientado a realizar a testagem e o isolamento social. A iniciativa apresenta uma boa efetividade na contensão da pandemia e protege os dados pessoais de seus usuários em um nível razoável, pois o processamento dos dados é realizado de forma local no celular.

No entanto, há a possibilidade de repasse à terceiros, no caso de pessoas doentes, além da atribuição dos números de telefone às informações cadastradas no app. Conforme foi visto, a arquitetura de *contact tracing* por *bluetooth* não necessita de qualquer tipo de cadastro dos usuários. As únicas informações essenciais são o número de identificação do celular que foi gerado pelo aplicativo, assim como a lista dos números que indicam quais aparelhos o usuário teve contato.

Na Índia, o sistema de combate a coronavírus sai diretamente de uma distopia orwelliana. O nível de monitoramento implementado pelo governo local excede todos os limites de necessidade, razoabilidade, proporcionalidade e finalidade, além da ausência de limitação temporal. O app desenvolvido viola o direito fundamental à privacidade, que foi reconhecido pela corte constitucional do país, pois o nível de vigilância implementado não é compatível com as prerrogativas de combate a uma crise de saúde pública. Os dados serão armazenados por tempo limitado, são extraídas informações que não possuem vínculo com o coronavírus, não há qualquer tipo de fiscalização ou transparência envolvida na arquitetura de funcionamento do aplicativo. O cenário é de grave violação aos diretos fundamentais e ao sistema de liberdades democráticas.

Por fim, é possível a construção de alternativas de vigilância digital que tenham efetividade epidemiológica e que sejam embasadas e limitadas de forma que proteja os dados pessoais dos titulares. As alternativas de *contact tracing* por meio de *checkpoints* e *bluetooth* são amigáveis aos direitos digitais, sendo a segunda alternativa mais eficaz e prática, estimulando a adesão e permanência dos usuários nos programas de controle da pandemia. A arquitetura desses *softwares* deve seguir uma série de princípios para evitar abuso de direitos e a transgressão às garantias fundamentais. Assim, se limitados a todas as condições, os direitos

à privacidade, à dignidade humana e à liberdade permanecem fortes nos mecanismos utilizados para combater a COVID-19.

REFERÊNCIAS BIBLIOGRÁFICAS

ABELER, Johannes; BÄCKER, Matthias; BUERMEYER, Ulf; ZILLESSEN, Hannah. COVID-19 Contact Tracing and Data Protection Can Go Together. **Jmir Mhealth And Uhealth**, [s.l.], v. 8, n. 4, p. 1-5, 20 abr. 2020. JMIR Publications Inc.. http://dx.doi.org/10.2196/19359. Disponível em: https://mhealth.jmir.org/2020/4/e19359/. Acesso em: 15 jun. 2020.

BBC. Coronavírus: **OMS declara pandemia**. 2020. Disponível em: https://www.bbc.com/portuguese/geral-51842518. Acesso em: 01 abr. 2020.

CENTER, Electronic Privacy Information. **The Code of Fair Information Practices**. 2020. Disponível em: https://epic.org/privacy/consumer/code_fair_info.html. Acesso em: 19 maio 2020.

DEB, Sidharth. **Privacy prescriptions for technology interventions on Covid-19 in India**. 2020. Coordenada por Internet Freedom Foundation. p. 1-88. Disponível em: https://drive.google.com/file/d/1UK5rElhcdP5T3Y-8fYP6cCgQKKpQBeOX/view. Acesso em: 25 maio 2020.

ESTADÃO. **Pelo terceiro dia seguido, SP tem mais de 5.500 novos casos de covid-19; mortes vão a 7.532**. 2020. Disponível em: https://saude.estadao.com.br/noticias/geral,pelo-terceiro-dia-seguido-sp-tem-mais-de-5500-novos-casos-de-covid-19-mortes-vao-a-7532,70003319919. Acesso em: 30 maio 2020.

EXPRESS. **Google Maps is tracking you! How your smartphone knows your every move**: a mapping device on a popular brand of smartphone keeps a record of each journey you take. 2014. Disponível em: https://www.express.co.uk/life-style/science-technology/500811/Google-Maps-is-tracking-your-every-move. Acesso em: 16 maio 2020.

FORBES. **Conheça o TraceTogether, app de monitoramento do coronavírus criado por Singapura**. 2020. Disponível em: https://forbes.com.br/negocios/2020/03/conheca-o-tracetogether-app-de-monitoramento-do-coronavirus-criado-por-singapura/. Acesso em: 27 maio 2020.

G1. **OMS esclarece que assintomáticos transmitem coronavírus: 'a questão é saber quanto'**. 2020. Disponível em: https://g1.globo.com/bemestar/coronavirus/noticia/2020/06/09/transmissao-por-casos-assintomaticos-esta-ocorrendo-a-questao-e-saber-quanto-diz-oms.ghtml. Acesso em: 09 jun. 2020.

GURUSWAMY, Menaka. Justice K.S. Puttaswamy (Ret'd) and Anr v. Union of India and Ors. **American Journal Of International Law**, [s.l.], v. 111, n. 4, p. 994-1000, out. 2017. Cambridge University Press (CUP). http://dx.doi.org/10.1017/ajil.2017.92. Disponível em: https://www.cambridge.org/core/journals/american-journal-of-international-

law/article/justice-ks-puttaswamy-retd-and-anr-v-union-of-india-and-ors/ED631B8F922039BEC5400086C8E34338. Acesso em: 15 jun. 2020.

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

INDIA, The Times Of**. India plans wristband patient surveillance as lockdown eases.** 2020. Disponível em: https://timesofindia.indiatimes.com/india/india-plans-wristband-patient-surveillance-as-lockdown-eases/articleshow/75300967.cms. Acesso em: 12 maio 2020.

KEESARA, Sirina et al. **Covid-19 and Health Care's Digital Revolution**. p. 1-3. Disponível em: https://www.nejm.org/doi/full/10.1056/NEJMp2005835. Acesso em: 22 maio 2020.

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. http://dx.doi.org/10.1038/d41586-020-01578-0.

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 jun. 2020.

POST, The Washington. **You downloaded FaceApp. Here's what you've just done to your privacy.** 2019. Disponível em: https://www.washingtonpost.com/technology/2019/07/17/you-downloaded-faceapp-heres-what-youve-just-done-your-privacy/. Acesso em: 15 jun. 2020.

ROCHER, Luc. **Estimating the success of re-identifications in incomplete datasets using generative models**. p. 1-9. Disponível em: https://www.nature.com/articles/s41467-019-10933-3. Acesso em: 08 jun. 2020.

TRACETOGETHER. **How is my data protected?** 2020. Disponível em: https://support.tracetogether.gov.sg/hc/en-sg/articles/360043234694-How-is-my-data-protected-. Acesso em: 08 jun. 2020.

TRACETOGETHER. TraceTogether **Privacy Safeguards**. Disponível em: https://www.tracetogether.gov.sg/common/privacystatement. Acesso em: 08 jun. 2020.

TRACETOGETHER. **What data is collected? Are you able to see my personal data?** 2020. Disponível em: https://support.tracetogether.gov.sg/hc/en-sg/articles/360043735693-What-data-is-collected-Are-you-able-to-see-my-personal-data-. Acesso em: 08 jun. 2020.

WEB, The Next**. India wants to build an ultra-intrusive 'wristband' to track coronavirus patients' every move**. 2020. Disponível em: https://thenextweb.com/in/2020/04/22/india-wants-to-build-an-ultra-intrusive-wristband-to-track-coronavirus-patients-every-move/. Acesso em: 13 maio 2020.

World Health Organization (org.). **Ethical considerations to guide the use of digital proximity tracking technologies for COVID-19 contact tracing**. 2020. Disponível em: https://www.who.int/publications/i/item/WHO-2019-nCoV-Ethics_Contact_tracing_apps-2020.1. Acesso em: 21 jun. 2020.

World Health Organization (org.). **WHO Coronavirus Disease (COVID-19) Dashboard**. Disponível em: https://covid19.who.int/. Acesso em: 28 mai. 2020.