2020 | ABRIL

# NOTA TÉCNICA

# USO DE DADOS DE GEOLOCALIZAÇÃO NO COMBATE AO COVID-19

## CONSIDERAÇÕES SOBRE PRIVACIDADE E TUTELA DA SAÚDE DURANTE A PANDEMIA

LAPIN

Considerando a proliferação de iniciativas que têm sido lançadas para **tratar dados de geolocalização**[1] **no combate ao COVID-19**,[2] o Laboratório de Políticas Públicas e Internet - LAPIN vem, por esta carta, apresentar suas considerações a respeito do uso dessa tecnologia pelo Estado, tendo em conta seus impactos à privacidade e à proteção de dados pessoais.

## I - Introdução

Na tentativa de conter a epidemia de COVID-19, o uso de dados de geolocalização tem sido feito por alguns países para monitorar o deslocamento de pessoas, identificar rotas de transmissão e impor distanciamento social. Majoritariamente, esse monitoramento é possibilitado pelo ecossistema de rastreamento que acompanha a precisão dos sensores de localização instalados em *smartphones*.

Um exemplo de aplicação dessa técnica foi feito pelo Ministério do Interior e Segurança da Coreia do Sul, que desenvolveu um aplicativo para celular destinado às pessoas que foram ordenadas a ficar em casa durante a epidemia. A ferramenta possibilita a esses indivíduos informarem o seu estado de saúde ao governo, que rastreia sua localização por GPS e verifica se o isolamento foi violado, buscando evitar, assim, que essas pessoas contaminem outras.[3] Foram

[1] Agência Brasil. VALENTE, Jonas. **Covid-19: iniciativas usam monitoramento e geram preocupações**, 12 abr. 2020. Disponível em https://agenciabrasil.ebc.com.br/geral/noticia/2020-04/covid-19-iniciativas-usam-monitoramento-e-geram-preocupacoes. Acesso em 13 abr. 2020.
[2] Agência Brasil. VALENTE, Jonas. **Governo usará dados de teles para monitorar circulação de pessoas**, 5 abr. 2020**.** Disponível em https://agenciabrasil.ebc.com.br/geral/noticia/2020-04/governo-usara-dados-de-teles-para-monitorar-circulacao-de-pessoas. Acesso em 8 abr. 2020.
[3] MIT Technology Review. ***South Korea is watching quarantined citizens with a smartphone app***. Disponível em https://www.technologyreview.com/2020/03/06/905459/coronavirus-south-korea-smartphone-app-quarantine/. Acesso em 08 de abr. 2020.

implementadas técnicas equivalentes em Taiwan, Israel[4], Singapura, Polônia e no Quênia.[5]

De forma similar, as autoridades de saúde pública dos Estados Unidos estão coletando dados sobre a localização da população, mas a partir de anunciantes online. O objetivo de evitar aglomerações de pessoas e estimar a adesão delas ao distanciamento social é o mesmo das iniciativas dos países mencionados anteriormente.[6]

Conforme veiculado pela mídia nacional, o governo federal tem avaliado a adoção de uma tática parecida em parceria com operadoras de telecomunicação. [7] As estratégias para o combate à disseminação do Coronavírus seriam desenvolvidas a partir do repasse de informações sobre a circulação de pessoas enquanto a epidemia não for controlada.

De acordo com o Sindicato Nacional das Empresas de Telefonia e de Serviço Móvel Celular e Pessoal (Sinditelebrasil), as informações repassadas possibilitariam o desenvolvimento de "mapas" para a visualização dos níveis de concentração de pessoas em determinados locais. O sindicato informou que os dados repassados seriam agregados e anonimizados, não sendo disponibilizados os nomes das pessoas e nem os seus números de linha.[8]

Apesar disso, não foram esclarecidos aspectos como quais procedimentos seriam adotados, por meio de qual técnica seriam tratados os dados, as finalidades

---

[4] CNBC. KHARPAL, Arjun. ***Use of surveillance to fight coronavirus raises concerns about government power after pandemic ends***, 26 mar. 2020. Disponível em https://www.cnbc.com/2020/03/27/coronavirus-surveillance-used-by-governments-to-fight-pandemic-privacy-concerns.html. Acesso em 9 abr 2020.

[5] ACCESS NOW. **Recommendations on Privacy and Data Protection on the Fight Against COVID-19**. [*S. l.*], 31 mar. 2020. Disponível em: https://www.accessnow.org/releases-recommendations-on-privacy-data-protection-covid-19/. Acesso em: 1 abr. 2020.

[6] The Wall Street Journal. ***Government Tracking How People Move Around in Coronavirus Pandemic.*** Disponível em https://www.wsj.com/articles/government-tracking-how-people-move-around-in-coronavirus-pandemic-11585393202. Acesso em 08 de abr. 2020.

[7] Agência Brasil, n. 1.

[8] SINDITELEBRASIL. **Operadoras vão disponilizar dados de mobilidade ao MCTIC para monitorar deslocamento**, 2 abr. 2020. Disponível em https://www.sinditelebrasil.org.br/sala-de-imprensa/releases/3375-operadoras-vao-disponilizar-dados-de-mobilidade-ao-mctic-para-monitorar-deslocamento. Acesso em 9 abr. 2020.

desses tratamentos e quais os agentes envolvidos no processo. No entanto, a três dias do lançamento oficial do programa, a iniciativa foi freada na esfera federal.[9]

Apesar da suspensão da medida em âmbito nacional, iniciativas locais já têm sido implementadas. É o caso do que o governo do Estado de São Paulo tem feito ao firmar parceria com empresas de telecomunicação. De acordo com comunicado do governo,[10] o Sistema de Monitoramento Inteligente de São Paulo (Simi-SP) surgiu a partir de parceria entre o governo estadual e as operadoras de telefonia Vivo, Tim, Oi e Claro.

A parceria "usa dados digitais para medir a adesão à quarentena em todo o Estado e também envia mensagens de alerta para regiões com maior incidência da COVID-19".[11]

Outra iniciativa ocorre na cidade de Recife, na qual a empresa In Loco, com atuação no oferecimento de soluções de negócios que usam dados de localização para estratégias de comunicação de marcas e engajamento de usuários com aplicativos, firmou parceria com a prefeitura de Recife.

A parceria pretende acompanhar casos e conter a propagação do vírus a partir da geolocalização de smartphones, acompanhando de forma coletiva o isolamento social e gerando índices de isolamento por bairro.[12]

Além desta parceria, a empresa adaptou seus serviços para realizar o monitoramento das medidas de isolamento social em âmbito nacional, tendo acesso à localização dos dispositivos que utilizem aplicativos parceiros da empresa[13]. O site da empresa apresenta política de privacidade com vários detalhes a respeito das técnicas de pseudonimização e anonimização utilizadas

---

[9] O GLOBO. Lauro Jardim. **Bolsonaro intervém e trava geolocalização via celular**. 13 abr. 2020. Disponível em: https://blogs.oglobo.globo.com/lauro-jardim/post/bolsonaro-intervem-e-trava-geolocalizacao-celular.html. Acesso em 13 abr. 2020.

[10] 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 13 abr 2020.

[11] Idem.

[12] 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 13 abr. 2020.

[13] 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: 13. abr. 2020.

para melhor proteger os dados de usuários. No entanto, não encontramos informações a respeito de quais seriam os aplicativos parceiros que estariam coletando esses dados.

As iniciativas implementadas no Estado de São Paulo e em Recife são alguns dos exemplos de aplicação de ferramentas de tratamento de dados pessoais para combater o COVID-19. Tendo em conta a proliferação desse tipo de ação pelo país, esta nota apresenta alguns dos pontos a serem endereçados no momento de desenho dessas políticas.

## II - Da necessidade de transparência

Ao implementar medidas de vigilância para o combate ao COVID-19, é necessário compreender de que maneira elas serão de fato eficientes para o fim almejado e quais salvaguardas serão desenvolvidas para evitar "efeitos colaterais" dos usos da medida, principalmente no que diz respeito à privacidade dos cidadãos. Neste contexto, implementar essas medidas com **transparência** é fundamental.

Dentre as informações a serem descritas, cabe aqui destacar:

1. Os **dados pessoais** coletados. Embora, no caso da ferramenta utilizada pelo Governo do Estado de São Paulo, se afirme que apenas a geolocalização é compartilhada, é importante se assegurar que este é mesmo o caso, uma vez que os registros de dados de chamada, que também são obtidos pelas operadoras, guardam diversas outras informações, tais como nome, endereço e dados financeiros, que não devem ser compartilhados neste contexto.

2. O **tipo de tecnologia de geolocalização** implementado. Existem duas técnicas comumente utilizadas:[14] o uso de torres de comunicação que geram os chamados *Cell Site Location*

[14] MCDONALD, Sean Martin. **Ebola: a Big Data Disaster.** India: The Centre for Internet and Society, 1 mar. 2016. Disponível em: https://cis-india.org/papers/ebola-a-big-data-disaster. Acesso em: 7 abr. 2020.

*Information* (CSLI), e o uso do *Global Positioning System* (GPS). A precisão de cada uma será descrita na seção V desta carta.

3. As **finalidades** almejadas. De acordo com notícias veiculadas na imprensa, os objetivos da medida, no Governo Federal, incluiriam rastrear: (i) a mobilidade populacional; (ii) deslocamentos; (iii) pontos de aglomeração; (iv) situações de concentração de pessoas; (v) risco de contaminação pelo novo coronavírus.[15] Já no Estado de São Paulo, por exemplo, o objetivo seria medir a adesão à quarentena e notificar indivíduos de regiões mais afetadas pelo vírus, uma medida que já poderia demandar a desanonimização do titular de dados. A esse respeito, o modelo apresentado pela In Loco em sua política de privacidade pode ser visto como modelo a ser seguido, ao descrever a finalidade específica para coleta de cada dado pessoal tratado pela empresa.[16]

4. A cadeia de **fluxo de dados** entre as entidades envolvidas. Embora se saiba que operadoras telefônicas - Algar Telecom, Claro, Oi, Tim e Vivo - estão envolvidas,[17] e, no caso do Governo Federal, também estaria a Microsoft, que seria responsável pela análise dos dados, não se sabe como ocorrerá a transmissão de dados entre esses diferentes agentes.[18] Apesar de haver maior detalhamento na proposta da In Loco a respeito de como é o funcionamento das transferências de dados entre diferentes operadores, falta referência a quais seriam os aplicativos parceiros da empresa.[19]

5. Quais salvaguardas de **proteção à privacidade** serão implementadas. Já foi veiculado pela mídia que técnicas de agregação e anonimização estão sendo utilizadas, mas não está

[15] 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 abr. 2020.
[16] IN LOCO. **Política de Privacidade: In Loco x COVID-19**. Op. Cit.
[17] SINDTELEBRASIL. **Operadoras vão disponilizar dados de mobilidade ao MCTIC para monitorar deslocamento.** [S. l.], 2 abr. 2020. Disponível em: https://www.sinditelebrasil.org.br/sala-de-imprensa/releases/3375-operadoras-vao-disponilizar-dados-de-mobilidade-ao-mctic-para-monitorar-deslocamento. Acesso em: 7 abr. 2020.
[18] VALENTE, Jonas. Op. Cit.
[19] IN LOCO. **Política de Privacidade: In Loco x COVID-19**. Op. Cit.

claro quais procedimentos serão adotados para implementação dessas técnicas e nem em qual momento do tratamento de dados isso será realizado. Além disso, seria interessante que os governos considerassem outros meios de garantir a privacidade de usuários e os publicizasse, como relatórios de impacto de proteção de dados. Isso especialmente pelo fato de que processos de anonimização não são completamente infalíveis, conforme será debatido mais à frente nesta carta.

Responder a essas perguntas é fundamental para que se garanta à sociedade a devida transparência a respeito de como o Estado está tratando seus dados. Isso vale não só para cumprir com preceitos de privacidade e proteção de dados, mas com o próprio direito de acesso à informação, regulado pela Lei n. 12.527/2020.

Neste sentido, **a observância da LGPD**, ainda que não esteja em pleno vigor, se mostra fundamental: a lei de proteção de dados autoriza o tratamento de dados pessoais para atender a políticas públicas (art. 7º, III), para a proteção da vida (art. 7º, VII) e para a tutela da saúde (art. 7º, VIII). Isto contudo deve ser feito com **respeito às diretrizes legais,** e em particular aos seus **princípios**. O papel desta lei no contexto do tratamento de dados para combater o COVID-19 será tratado na seção seguinte.

## III - Da proteção de dados pessoais

O primeiro princípio da LGPD que cabe aqui ser destacado por ser essencial em toda cadeia de tratamento de dados, desde sua coleta e armazenamento até seu descarte, é o já citado princípio da **transparência (art. 6º, VI)**, que deve permear inclusive o desenvolvimento do algoritmo.[20] Apesar disso, a falta de informações oficiais a respeito de como será realizado o

[20] FERRETTI, Luca; WYMANT, Chris, et. al. **Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing**. Science. 31 mar. 2020. Disponível em https://science.sciencemag.org/content/early/2020/03/30/science.abb6936.full. Acesso em 12 abr. 2020.

tratamento de dados fomenta[21] o cenário de incerteza já existente pelas várias incógnitas sobre sua utilização para conter a proliferação do vírus.

Seguir o princípio da **finalidade** também é indispensável. É ele que prevê que todo tratamento de dados pessoais deve ser feito de acordo com propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades.

Esse tipo de conduta é essencial inclusive para nortear a própria ação do poder público com esses dados, de modo a evitar que uma quantidade imensa de informações sejam coletadas sem uma noção exata do que será feito com ela.

Nesse sentido, a falta de finalidade clara pode levar a consequências negativas à sociedade: durante o surto do Ebola na África ocidental, o monitoramento por geolocalização não foi capaz de rastrear a rota de contaminação do vírus, pois a precisão das tecnologias utilizadas (CSLI e GPS) era inferior ao necessário para alcançar o objetivo almejado. Desta forma, a ausência de uma análise técnica apropriada prejudicou a efetividade da medida, enquanto, em contrapartida, a privacidade de cidadãos de países africanos foi comprometida.[22]

Dois outros princípios expressos na lei são o da **adequação** (art. 6º, II) e da **necessidade** (art. 6º, III). Eles prescrevem respectivamente que o tratamento seja compatível com as finalidades descritas e que seja limitado ao mínimo necessário para a realização de suas finalidades.

Levando em consideração esses princípios, as entidades envolvidas devem assegurar que **apenas os dados pessoais estritamente necessários sejam compartilhados entre si.** Ao que tudo aponta no caso em questão, estes seriam apenas os dados de geolocalização, sem a identificação por códigos fixos dos usuários, como IMEI e MAC.

O controlador também deve **manter esses dados armazenados pelo mínimo tempo possível** necessário à finalidade almejada pelo controlador (*storage limitation*). Uma vez alcançada esta finalidade, devem ser descartados, salvo possibilidade de aplicação de uma das exceções contidas no art. 16 da LGPD,

[21] DIEB, D.; GOMES, H. S. Op. cit.
[22] MC DONALD, S. M.. (n 2).

que obriga o controlador a eliminar dados pessoais após o término de seu tratamento.

As exceções são para os casos em que precisa cumprir obrigação legal ou regulatória, para fins de pesquisa, transferência a terceiros (desde que com base nos requisitos da LGPD) ou para seu uso exclusivo, desde que anonimizados os dados.

No que diz respeito à categorização desses dados para fins de interoperabilidade dentro da administração pública federal, caso o poder público decida implementar o rastreamento de geolocalização, deve-se, em observância ao Decreto nº 10.046/2019, classificar os dados como pertencentes à **da categoria específica de compartilhamento**, de acordo com a categorização específica do prevista em seu artigo 4º, III[23]. Isso porque tratam de informações críticas, capazes de trazer problemas graves para seus titulares ou para o órgão caso sejam utilizadas de maneira indevida.[24]

Ao atribuí-los esta categoria, estes dados necessitarão de **expressa autorização do gestor dos dados para o compartilhamento** com demais órgãos e acessos. Nesse sentido, ainda que compartilhados, **não poderão ser retransmitidos** pela entidade que recebê-los, salvo por previsão expressa no ato de compartilhamento pelo gestor dos dados ou por autorização posterior. Vale ressaltar que o decreto supramencionado somente se aplica ao compartilhamento de dados entre entes da administração pública[25]

Outro ponto a ser considerado é que esses dados devem ser **compartilhados somente com órgãos diretamente envolvidos no combate ao COVID-19**, como autoridades sanitárias, pesquisadores e criadores de políticas públicas de saúde, de modo a garantir que as finalidades estipuladas para seu

---

[23] Art. 4º. O compartilhamento de dados entre os órgãos e as entidades de que trata o art. 1º é categorizado em três níveis, de acordo com sua confidencialidade:
III - compartilhamento específico, quando se tratar de dados protegidos por sigilo, nos termos da legislação, com concessão de acesso a órgãos e entidades específicos, nas hipóteses e para os fins previstos em lei, cujo compartilhamento e regras sejam definidos pelo gestor de dados.

[24] MINISTÉRIO DA ECONOMIA/SECRETARIA ESPECIAL DE DESBUROCRATIZAÇÃO, GESTÃO E GOVERNO DIGITAL (Brasil). Resolução nº 2, de 16 de março de 2020. **Dispõe sobre as orientações e as diretrizes para a categorização de compartilhamento de dados**, Brasília, DF, 20 mar. 2020.

[25] Art. 1º, § 1º. O disposto neste Decreto não se aplica ao compartilhamento de dados com os conselhos de fiscalização de profissões regulamentadas e com o setor privado.

tratamento se restrinjam ao combate à pandemia. Além disso, a supervisão constante do sistema por uma **autoridade independente** é indispensável.[26]

## IV - Da anonimização dos dados pessoais

Como ressaltado na seção anterior, os dados a serem tratados pelo governo passarão supostamente por um procedimento de anonimização por agregação. Caso assim seja, os dados perderão sua qualidade de dados pessoais, o que afastaria a incidência dos princípios da LGPD.

No entanto, é preciso entender **em que momento esses dados serão anonimizados.** Isso é fundamental para determinar o grau de exposição dos dados e a respectiva responsabilidade a se destinar a seu controlador ou operador.

Nesse sentido, as seguintes dúvidas são pertinentes: no caso do Governo do Estado de São Paulo, por exemplo, que utilizará dados cedidos por operadoras de telefonia, estas já compartilhariam esses dados em formato anonimizado? Existem dados sendo enviados para análise por parceiros internacionais?

Caso a última resposta seja positiva, é importante observar se as legislações dos países estrangeiros oferecem proteções adequadas, ou se as empresas contratadas estabelecem uma política de privacidade compatível com a legislação brasileira.

Ademais, é importante ter em mente que **dados de geolocalização de celular anonimizados são facilmente re-identificáveis.** Foi o que concluiu estudo realizado pelo MIT (EUA) e pela UCL Louvain (BE) em 2013,[27] ao revelar que 4 pontos de geolocalização foram suficientes para revelar a identidade de 95% dos indivíduos.

Esse **risco pode ser reduzido se os dados forem devidamente agregados.** Se não ocorrer dessa forma, todos os controladores/operadores de

[26] FERRETTI, WYMANT et al. Op. cit.
[27] DE MONTJOYE, Yves-Alexandre; HIDALGO, César A.; VERLEYSEN, Michel; BLONDEL , Vincent D. **Unique in the Crowd: The privacy bounds of human mobility.** [S. l.]: Nature, 25 mar. 2013. Disponível em: https://www.nature.com/articles/srep01376#ref20. Acesso em: 7 abr. 2020.

dados que possuírem esses dados serão capazes de re-identificar seus titulares sem muita dificuldade.

Nesse cenário, não haverá sequer como se falar em **anonimização nos termos da LGPD,** já que essa, em seu art. 5º, III define o conceito como o **processo pelo qual o titular dos dados perderia a capacidade de ser identificado**. Seria, portanto, mais adequado referir-se a esses dados como **pseudoanonimizados**, o que requer maiores salvaguardas à privacidade e à proteção de dados desses indivíduos. A solução apresentada pela In Loco a ser aplicada em Recife, por exemplo, usa ambas as técnicas.[28]

Conforme descrito por Finck e Pallas,[29] a anonimização deve ser entendida como um meio de reduzir o risco de identificação de titulares de dados. Embora nunca seja absoluta, a anonimização apenas ocorrerá se puder garantir que, em um determinado período, os recursos técnicos e financeiros então existentes tornariam o processo de re-identificação impraticável ou excessivamente dispendioso.

Ou seja, **a anonimização só existe se o risco de re-identificar um indivíduo for residual e irrelevante.** Baseado nessa abordagem, a agregação é apenas mais uma técnica (embora bastante relevante neste contexto) para garantir a anonimização dos dados.

Vale ressaltar que, após a conclusão do propósito almejado com o tratamento, o descarte dos dados coletados deve ocorrer de maneira segura, e, caso sejam armazenados para propósitos científicos ou estatísticos, devem passar pelo processo correto de anonimização (caso não tenham sido anteriormente), devendo **todos dados não agregados ser eliminados**[30]. Isso deveria ocorrer, preferencialmente, logo depois que a pandemia for declarada superada pelas autoridades de saúde globais.

---

[28]IN LOCO. Política de Privacidade: In Loco x COVID-19. Op. Cit.

[29] FINCK, Michèle; PALLAS, Frank. **They who must not be identified—distinguishing personal from non-personal data under the GDPR**. International Data Privacy Law, Oxford, p. 1-26, 10 mar. 2020. Disponível em: https://github.com/DP-3T/documents/blob/master/DP3T%20White%20Paper.pdf. Acesso em: 9 abr. 2020.

[30] ACCESS NOW. **Recommendations on Privacy and Data Protection on the Fight Against COVID-19**. [*S. l.*], 31 mar. 2020. Disponível em: https://www.accessnow.org/releases-recommendations-on-privacy-data-protection-covid-19/. Acesso em: 1 abr. 2020.

## V - Considerações sobre a eficiência da geolocalização

Como ressaltado na seção II, com base nas informações veiculadas pelo Sinditelebrasil e pela imprensa a respeito das intenções do governo brasileiro em coletar dados de geolocalização, pode-se presumir que essa coleta aconteça de duas formas: por CSLI ou GPS.

Enquanto o CSLI possui uma acurácia que pode variar de 2km a 5km, que pode ser vista como altamente imprecisa para medir tanto o contato necessário entre pessoas para transmissão do vírus quanto se um indivíduo está de fato cumprindo a quarentena, o GPS pode ter uma precisão de 1,6m a 5m.[31]

Por terem graus de precisão muito distintos, as finalidades a serem buscadas deverão também ser diversas. Considerando que o contágio de COVID-19 exige (i) o contato físico com uma pessoa ou superfície contaminada e (ii) a aproximação com um indivíduo contaminado a uma distância média de 1,5m,[32] a conclusão a que se chega é que a geolocalização por CSLI é deveras imprecisa e portanto ineficaz em alcançar o objetivo de identificar se um indivíduo teve contato com alguém contaminado.

No que tange ao GPS, sua maior precisão torna a ferramenta mais efetiva para medir a distância entre pessoas e o deslocamento de cada uma delas. Apesar disso, a tecnologia também encontra obstáculos expressivos. O primeiro deles é o fato de que GPS encontra falhas ao buscar localizar indivíduos em locais fechados, como o metrô ou um supermercado.[33] Por isso, monitorar a distância

---

[31] LODE, Eric. **Cell Phone Location Tracking.** United States: University of Berkeley, 7 jun. 2016. Disponível em: https://www.law.berkeley.edu/wp-content/uploads/2015/04/2016-06-07_Cell-Tracking-Primer_Final.pdf. Acesso em: 7 abr. 2020.

[32] De acordo com o Centers for Disease Control and Prevention (CDC), órgão de controle e prevenção de doenças dos Estados Unidos, a transmissão ocorre entre uma pessoa e outra quando estão a uma distância de até 1,82m. Vide Centers for Disease Control and Prevention (CDC). **How COVID-19 Spreads**. Disponível em https://www.cdc.gov/coronavirus/2019-ncov/prevent-getting-sick/how-covid-spreads.html?CDC_AA_refVal=https%3A%2F%2Fwww.cdc.gov%2Fcoronavirus%2F2019-ncov%2Fprepare%2Ftransmission.html. Acesso em 7 abr. 2020.

[33] 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 abr. 2020.

entre pessoas pode ter sua precisão largamente afetada pelas fraquezas dessa técnica. A esse respeito, vale ressaltar a opinião de Horst Kapfenberger, cientista da computação da ONG *noyb*, que afirma que, devido à sua imprecisão, dados de geolocalização de provedores de telefonia são inadequados a determinar possíveis infecções pelo coronavírus.[34]

Além disto, não há garantias que o GPS será capaz de rastrear a proliferação do virus, como o exemplo já citado do combate ao Ebola na África Oriental. Conforme reportado,[35] não foram levantadas evidências científicas (sequer após a crise epidêmica) de que a geolocalização foi capaz de rastrear de forma eficaz a rota de transmissão do vírus.

Isto não significa, no entanto, que o GPS será sempre ineficiente: caso o fim almejado seja identificar aglomerações, através da emissão de "ondas de calor", uma precisão de até 5m é mais que suficiente. Porém, rastrear rotas exatas de proliferação do vírus dificilmente seria eficaz com o uso de geolocalização, e poderia levar a um excesso de notificações de indivíduos supostamente contaminados, o que poderia sobrecarregar ainda mais o sistema de saúde.

A **garantia da qualidade e precisão dos dados** tratados é fundamental para que sua utilização contra a proliferação do COVID-19 seja eficiente e gere conclusões assertivas. Aqui, mais uma vez, é necessário que se tenha em mente a finalidade exata para que os dados serão tratados para evitar que pessoas passem a receber uma avalanche de notificações que não têm o grau de precisão adequado.

A qualidade dos dados deve levar em conta também a forma de contato que houve entre determinado par de pessoas para identificar a probabilidade de um contágio. Caso o objetivo da coleta de dados pelo governo seja rastrear contágios, cenários realistas para o rastreamento de infecções são, por exemplo, o encontro entre pessoas em uma viagem de trem ou ônibus, ou interações longas entre pessoas em loja ou restaurante.

Por outro lado, determinar quarentena a uma pessoa por meramente passar por alguém contagiado em uma rua, ou identificar pessoas que trabalham

---

[34] Noyb. **Data protection in times of coronavirus: not a question of if, but of how**. 30 mar 2020. Disponível em https://noyb.eu/en/data-protection-times-corona. Acesso em 8 abr. 2020.

[35] MC DONALD, N. M. Op. cit., p. 34.

ou moram com alguém infectado são de pouca valia. Isso porque, no primeiro caso, torna-se difícil mensurar como foi dado o contato entre esses indivíduos e se ele foi de fato suficiente para consolidar uma suspeita de contágio. No segundo, porque essas pessoas que convivem com o infectado provavelmente já sabem de seu contágio de qualquer forma, sem precisar de uma análise de dados de geolocalização para isso.[36]

Isso demonstra como cada tecnologia tem seus pontos fortes e fracos para cada um desses cenários. Por isso é que transparência e o devido planejamento das finalidades a serem obtidas são de tamanha importância.

## VI - Uma possível alternativa: *bluetooth*

Outras tecnologias também podem ser usadas para localizar indivíduos de forma menos intrusiva em sua privacidade. Uma delas é o *bluetooth*, que é inclusive recomendada por um grupo de pesquisadores da Universidade Federal de Santa Catarina, que estão desenvolvendo um aplicativo móvel para coletar os encontros físicos entre pessoas, através de identificadores anônimos. De acordo com comunicado que divulga solução proposta pelo grupo, seriam "armazenados apenas dados relativos aos encontros entre bluetooths, a data, a distância, e a duração deles".[37]

Apesar disso, a tecnologia também tem pontos fracos em relação à privacidade dos usuários. Quando tem o *bluetooth* ligado, o celular emite sinais à vizinhança em intervalos de até 10 segundos. A partir desses sinais, que têm raio de alcance de normalmente 10m, mas que pode chegar a 100m, outros aparelhos podem identificar a presença do celular que originou o sinal. Essa técnica foi usada, por exemplo, pelo governo da Singapura, com o aplicativo TraceTogether.[38]

---

[36] Noyb. **Ad hoc Paper (V0.2) SARS-CoV-2 Tracking under GDPR.** 29 mar. 2020, p. 1. Disponível em https://noyb.eu/sites/default/files/2020-04/Ad%20hoc%20Paper_Corona%20Tracking_v0.2.pdf. Acesso em 8 abr. 2020.

[37] UFSC, Departamento de Informática e Estatística. **Força tarefa de professores da Computação da UFSC, desenvolvedores voluntários e um grupo europeu, na corrida contra o coronavírus.** Disponível em https://ine.ufsc.br. Acesso em 7 abr. 2020.

[38] Privacy International. **Bluetooth tracking and COVID-19: A tech primer.** 31 março 2020. Disponível em

Nesse sentido, o rastreamento via *bluetooth* pode ser menos intrusivo ao se considerar que ele não se baseia no acompanhamento de uma pessoa, mas sim em suas interações com outros celulares. No entanto, pode ainda violar a privacidade do indivíduo pelo fato de que, ao emitir esses sinais frequentes, o aparelho pode ser rastreado por qualquer pessoa que interceptar seu sinal dentro de seu raio de alcance, já que, por esses sinais, pode-se rastrear dados individualizantes como o endereço MAC do celular.[39]

Uma forma de pseudo-anonimizar esse sinal é exigir que o controlador de dados não armazene os dados do endereço MAC seu celular, mas de um código pseudo-aleatório UUID (*Universally Unique Identifier*). Esse código também pode ser rastreável, mas permite a possibilidade de ser constantemente regenerável pelo controlador de dados. Essa regeneração dificultaria em grande medida a identificação do titular de dados.[40]

No momento, um modelo descentralizado de rastreamento da propagação do vírus por meio de *bluetooth,* que ao mesmo tempo garanta segurança e privacidade, vem sendo investigado por diversos especialistas. Em 8 de abril, cientistas de diversas universidades renomadas, incluindo Oxford (Reino Unido), KU Leuven (Bélgica), TU Delft (Holanda), TU Berlin (Alemanha) e ETHZ (China), apresentaram uma publicação onde apresentam uma proposta de solução. Por ela, contatos entre dispositivos seriam identificados sem utilizaria dados de geolocalização. Além disso, a plataforma geraria identificadores provisórios para evitar que usuários fossem rastreados e deixaria de funcionar assim que a pandemia fosse declarada extinta.[41]

Solução semelhante tem sido buscada por meio de parceria entre Google e Apple[42]. As empresas anunciaram o desenvolvimento de uma plataforma que

---

https://privacyinternational.org/explainer/3536/bluetooth-tracking-and-covid-19-tech-primer. Acesso em 7 abr 2020.

[39] *Idem*.

[40] *Ibidem*.

[41] EPFL; ETHZ; KU LEUVEN; TU DELFT, UNIVERSITY COLLEGE LONDON, CISPA, UNIVERSITY OF OXFORD, TU BERLIN, UNIVERSITY OF TORINO. **Decentralized Privacy-Preserving Proximity Tracing**. [S. l.], 8 abr. 2020. Disponível em: https://github.com/DP-3T/documents/blob/master/DP3T%20White%20Paper.pdf. Acesso em: 9 abr. 2020.

[42] Apple. **Apple and Google partner on COVID-19 contact tracing technology**. 10 abr. 2020. Disponível em https://www.apple.com/newsroom/2020/04/apple-and-google-partner-on-covid-19-contact-tracing-technology/. Acesso em 12 abr. 2020.

utiliza *bluetooth* para identificar contatos entre pessoas sem usar seus dados de localização, mas apenas de reconhecimento de outros aparelhos em suas proximidades. Cada indivíduo teria a oportunidade de optar por ter suas interações identificadas ou não por um mecanismo de *opt-in*, e seriam gerados identificadores provisórios a cada 15 minutos, para dificultar o rastreamento de seu aparelho.[43]

Embora algumas propostas já estejam em andamento pelo país, é importante que o poder público acompanhe a evolução dessas pesquisas, já que soluções práticas podem surgir rapidamente em um contexto em que toda a comunidade técnico-científica internacional junta esforços para o combate da pandemia.

## VII - Conclusão

Com base no exposto, é necessário que as medidas a serem implementadas pelos governos e empresas para tratamento de dados de geolocalização sejam devidamente explicadas aos cidadãos, com base nos prismas indicados: **transparência, necessidade, proporcionalidade e adequação**, esta última incluindo, principalmente, a possibilidade de acesso aos dados pessoais por seus titulares.

A exposição das finalidades buscadas também é essencial para que se possa definir o tipo de técnica de tratamento de dados a ser implementado. Como visto, geolocalização por CSLI não parece uma técnica adequada para identificar contaminações individuais. No entanto, pode ser eficaz para determinar fluxos de contaminação de um bairro a outro ou de uma cidade a outra, por exemplo.

O GPS também possui suas limitações, especialmente para considerar contatos em ambientes fechados, que são os mais propensos a motivar contaminações por COVID-19. A identificação de aproximação via *bluetooth*

[43] Apple & Google. **Contact Tracing, Bluetooth Specification.** 10 abr. 2020. Disponível em https://covid19-static.cdn-apple.com/applications/covid19/current/static/contact-tracing/pdf/ContactTracing-BluetoothSpecificationv1.1.pdf. Acesso em 12 abr. 2020.

apresenta-se como a alternativa menos intrusiva, mas até mesmo ela pode levar a riscos à segurança e à privacidade de usuários.

Vale ressaltar que a postura de coletar dados sem uma definição clara de finalidade pode não só reduzir a confiança de cidadãos no governo, mas também levar a novas contaminações. Afinal, se o número de falsos positivos (pessoas erroneamente identificadas como expostas ao COVID-19) e falsos negativos (pessoas expostas que não foram identificadas pelo sistema) for significativo, pessoas não contaminadas serão dirigidas aos hospitais enquanto as que deveriam ser isoladas não o serão.[44] Além disso, o rastreamento eficiente da rota de propagação do vírus ficará comprometido.

Os governos também devem estar cientes das últimas pesquisas sobre o tema, de modo a identificar a tecnologia mais efetiva para os fins buscados e que ao mesmo tempo garanta a privacidade dos cidadãos. Os exemplos de soluções buscadas com o uso de *bluetooth* são alguns a serem observados pelo poder público brasileiro como soluções possivelmente menos invasivas.

Sobretudo, deve-se ter em mente o fato de que processos de anonimização nunca são completamente irreversíveis.[45] Por isso, é necessário que todos os meios ao alcance das entidades envolvidas sejam aplicados para evitar a identificação das pessoas cujos dados estão sendo tratados no combate ao COVID-19. Com isso, será reduzido em muito o risco de que tanto invasores quanto os próprios agentes de tratamento desses dados (controladores e operadores) consigam reverter a anonimização, nos termos do art. 5º, III, da LGPD.

Isto posto, o LAPIN reforça a necessidade de que governos e empresas apresentem informações precisas a respeito do tratamento de dados de geolocalização para fins de combate ao COVID-19. Afinal, a tutela da saúde e a proteção da privacidade não são conceitos excludentes, mas complementares, de modo a proteger os direitos de indivíduos durante e após a crise que assola o mundo.

---

[44] *Idem*, supra, LANDAU, 2020.
[45] FINCK, M; PALLAS, F. Op. cit., p. 25.

**ANEXO -** Tabela comparativa entre modelos adotados em São Paulo e Recife

| | São Paulo | Recife |
|---|---|---|
| **Limite de armazenamento de dados** | Sem previsão. | Dois anos |
| **Dados coletados** | Não há descrição exata a respeito dos dados coletados. | • GPS<br>• Sinais de Wi-Fi<br>• Sinais de Bluetooth<br>• Sinais de telefone e atividades<br>• Modelo do aparelho<br>• Sistema operacional<br>• Versão do SO<br>• Métricas de performance do SDK<br>• IP (sendo os últimos 4 dígitos ignorados para remover precisão)<br>• Tipo de rede (3G, 4G, Wi-Fi)<br>• Provedor de rede<br>• Resolução da tela |
| **Finalidades do tratamento de dados** | Medir adesão à quarentena e enviar mensagens de alerta para regiões com maior incidência da COVID-19 | • Envio de alerta de proximidade a locais de risco<br>• Contagem de visitas<br>• Análise de mobilidade<br>• Envio de campanhas educativas<br>• Segmentação<br>• Contagem de usuários únicos<br>• Métricas de performance de campanha<br>• Depuração e monitoramento do SDK<br>• Otimização de recursos de rede<br>• Segmentação para excluir informações de regiões que não serão analisadas<br>• Bloquear coleta de dados de menores de idade (<18 anos)<br>• Inteligência sobre uso de apps<br>• Avaliação da comunicação através de notificações push |

| | | |
|---|---|---|
| **Técnicas de segurança** | Menciona apenas a utilização de anonimização por agregação, sem fornecer detalhes a respeito do momento em que ocorrerá a anonimização ou como serão feitos os alertas | Anonimização por agregação, *hash*, criptografia, consolidação de dados em *clusters* e disponibilização de *opt out* |
| **Empresas envolvidas** | Vivo, Claro, Oi e Tim | In Loco e aplicativos associados (não menciona quais seriam esses) |
| **Formas de monitoramento** | Consulta de informações georreferenciadas de mobilidade urbana em tempo real em municípios paulistas de mais de 30 mil habitantes e em bairros das cidades mais populosas e criação de mapas de calor de aglomeração | Criação de mapa demonstrativo do percentual da população que está respeitando as recomendações de isolamento pela coleta de dados dos aplicativos associados |