

A UTILIZAÇÃO DE DADOS DE GEOLOCALIZAÇÃO NO COMBATE À PANDEMIA DO CORONAVÍRUS - A necessidade de adoção de salvaguardas regulatórias

Demócrito Reinaldo Filho

Desembargador do TJPE

Em artigo anterior, descrevemos como os países asiáticos estão combatendo de forma eficaz os efeitos da pandemia do coronavírus, através do uso da tecnologia. Apostaram fortemente na vigilância digital e na utilização de *Big Data* e inteligência artificial. A China construiu um enorme aparato de vigilância, um sistema formado por 200 milhões de câmeras de vídeo, com software de reconhecimento facial, que controlam o movimento das pessoas. Por meio do material filmado pelas câmeras e de dados de localização fornecidos pelos provedores de serviços na Internet e operadoras de telefonia é possível criar o perfil de movimento completo de um infectado e avisar as pessoas que com ele tiveram contato¹.

É óbvio que não se vai defender a replicação, em países de tradição libertária e democrática, do modelo chinês de vigilância digital, que representa uma séria ameaça para a privacidade dos indivíduos. Mas para maior sucesso no enfrentamento da pandemia, é indispensável recorrer a algumas ferramentas tecnológicas, que permitem a

¹ COMO OS PAÍSES ASIÁTICOS UTILIZAM A TECNOLOGIA PARA COMBATER A EPIDEMIA DO CORONAVÍRUS - A transição do "capitalismo de vigilância" para a "vigilância totalitária"?, artigo publicado no site Juristas, em 25.03.20, acessível em: <https://juristas.com.br/2020/03/25/pandemia-coronavirus/>

coleta de dados de geolocalização. O uso dessa categoria de dados permite acompanhar a velocidade com que o vírus se espalha por determinadas áreas, bem como identificar regiões com mais risco para o contágio.

A forma mais eficaz de combater a propagação da pandemia do coronavírus, como reconhecido pela Organização Mundial da Saúde (OMS), é através do rastreamento dos contatos. Mesmo o Brasil já tendo ingressado na fase da "transmissão comunitária" do vírus, ainda assim o rastreamento de aparelhos celulares pode ser útil. Existe um gigantesco banco de dados, capaz de fornecer informação pontual sobre onde estávamos em um determinado momento. Esse banco de dados é gerado diariamente pelos nossos telefones celulares. Por meio do monitoramento dos aparelhos móveis de telefonia, podem ser levantados os dados de deslocamento, não apenas do momento atual. É possível reconstruir "gráficos geográficos", que indicam por onde as pessoas transitaram em períodos de tempo pretéritos.

Esses dados que permitem geolocalizar usuários de aparelhos celular estão em poder das operadoras de telefonia e das grandes empresas de tecnologia que prestam serviços na Internet. Ao invés de construir regimes de vigilância à semelhança do aparato chinês, governos de países democráticos podem se utilizar dos dados coletados e armazenados por essas empresas, para o desenvolvimento de políticas públicas de combate a epidemia do coronavírus. Ferramentas de controle de contágio podem ser desenvolvidas, não com a ideologia de controle ou domínio social, mas para salvar vidas. A utilização de dados de geolocalização pode ser legitimada para um monitoramento e controle da expansão da epidemia, desde que isso resulte na preservação da vida humana e sejam respeitadas determinadas garantias individuais.

Por ser um valioso instrumento para acompanhar o ritmo da expansão do vírus e mesmo para controlá-lo, países ocidentais e diversos governos de democracias capitalistas também estão utilizando ou planejando utilizar desses dados. Em Israel, usuários de *smartphones* já recebem alertas sobre a aproximação de pessoas possivelmente infectadas com o coronavírus. No dia 18 deste mês, cerca de 400 pessoas receberam uma notificação com alerta de que estavam próximas de pessoa com resultado positivo para o vírus. A mensagem aconselhava a se isolarem por 14 dias, para proteger outras pessoas do contágio².

Na Inglaterra e nos EUA, as autoridades governamentais estão negociando com as grandes empresas de tecnologia. O governo inglês está requisitando dados anônimos de localização de celulares para ver se as pessoas estão seguindo as determinações de distanciamento social. As autoridades daquele país acreditam que podem, através desses dados, saber se os cidadãos ingleses estão cumprindo as diretrizes de quarentena e as restrições ao transporte de pessoas. Nos EUA, o Presidente Trump já se reuniu com representantes da Google, Facebook, Apple, Amazon e IBM para ter acesso aos dados de localização. A ideia é utilizar esses dados para fazer um monitoramento das pessoas, de modo a garantir que mantenham uma distância segura entre elas³. Com certo atraso, depois de a epidemia ter se alastrado e causado a morte de milhares de pessoas (sobretudo na Itália e na Espanha), a Comissão Europeia

² Ver reportagem publicada no site *Olhar Digital*, no dia 20.03.20, sob o título "Para combater o coronavírus, governos querem dados de localização", acessível em: <https://olhardigital.com.br/coronavirus/noticia/para-combater-o-coronavirus-governos-querem-dados-de-localizacao/98356>

³ Ver reportagem publicada no jornal *Washington Post*, no dia 17.03.20, sob o título "U.S. government, tech industry discussing ways to use smartphone location data to combat coronavirus", acessível em: <https://www.washingtonpost.com/technology/2020/03/17/white-house-location-data-coronavirus/>

tomou a iniciativa de requisitar dados de localização aos provedores europeus de telefonia, numa tentativa de combater a evolução do coronavírus no continente⁴. Alguns países do bloco europeu já tinham, de forma não regulada e isolada, feito acordos com os provedores de Internet, para ter acesso a esses dados⁵. Agora a Comissão Europeia resolveu tomar iniciativa coordenada e com a supervisão da Autoridade Europeia para a Proteção de Dados.

No Brasil ainda não se tem notícia de que o Governo federal tenha adotado políticas públicas de contenção e controle do vírus através do monitoramento de celulares. Entretanto, dois municípios saíram na frente e estão adotando tecnologias que identificam o padrão de movimento das pessoas, para mapear a propagação da infecção. A Prefeitura do RJ fechou uma parceria com a operadora TIM para rastrear celulares. O sistema permite acompanhar as concentrações e movimentos de pessoas nos territórios afetados pela pandemia. A TIM afirma que o sistema de análise de dados de deslocamento da população é o mesmo que vem utilizando na Itália e em outros países europeus para o combate à proliferação do coronavírus. São utilizados dados em tempo real, que identificam a concentração de usuários em um determinado momento e, assim, permite entender a movimentação pela cidade e se as medidas de isolamento estão sendo eficazes. A TIM garante que todas as informações coletadas são anônimas, respeitando-se critérios de confidencialidade e segurança dos dados⁶. A Prefeitura do Recife também adotou

⁴ Ver reportagem sob o título "Coronavírus: operadoras passam a rastrear localização de celulares na Europa", publicada no site *Olhar Digital*, no dia 26.03.20, acessível em:

<https://www.tudocelular.com/seguranca/noticias/n154217/operadoras-rastreiam-localizacao-celulares-europa.html>

⁵ Ver notícia publicada no dia 20.03.20, acessível em:

<http://www.ihu.unisinos.br/78-noticias/597285-coronavirus-os-governos-europeus-pedem-socorro-as-big-tech-mas-o-tempo-dos-mapas-de-contagio-esta-se-esgotando>

⁶ Ver reportagem sob o título "TIM fecha parceria com Prefeitura do Rio para rastrear movimento e combater vírus", publicada em no site *Olhar Digital*, no

iniciativa semelhante. Através de parceria com uma empresa privada local, está rastreando celulares e acompanhando o movimento de aproximadamente 700 mil pessoas diariamente. Segundo a Prefeitura, não há risco de invasão à privacidade, pois o monitoramento é apenas dos dispositivos móveis, já que os dados coletados não expõem a identidade dos proprietários. A ferramenta permite verificar se a política de isolamento social está sendo descumprida e, quando isso ocorre, são enviadas mensagens para os celulares para reforçar as medidas de segurança contra o coronavírus⁷.

Antes de fazer uma análise mais detida, de um ponto de vista legal, dessas iniciativas de monitoramento para combater a epidemia do coronavírus, é importante entender como os dados de geolocalização são recolhidos pelas operadoras de telefonia e empresas de tecnologia.

As operadoras de telefonia móvel conseguem obter os dados realizando a triangulação de células (antenas) da rede de telefonia móvel. Por esse meio, são capazes de saber, por exemplo, os números de telefones celulares de pessoas que transitaram por determinada área em específico período de tempo, por meio das coordenadas de latitude e longitude das torres (antenas) próximas. O processo de localização por triangulação de células permite revelar o local em que um usuário da rede de telefonia móvel estava em determinado momento. Os dados de localização aparecem em razão dos registros que apontam em qual antena (torre de celular) o equipamento estava conectado em determinado momento. Com a triangulação em

dia 23.03.20, acessível em: <https://www.infomoney.com.br/economia/tim-fecha-parceria-com-prefeitura-do-rio-para-rastrear-movimento-e-combater-virus/>

⁷ Conforme notícia publicada no portal G1, da Globo.com, em 24.03.20, acessível em: <https://g1.globo.com/pe/pernambuco/noticia/2020/03/24/recife-rastreia-700-mil-celulares-para-monitorar-isolamento-social-e-direcionar-acoess-contracoronavirus.ghtml>

tempo real, a operadora pode apontar o local exato de um aparelho, e ainda acompanhá-lo à medida que se move.

As empresas de tecnologia, provedoras de serviços na Internet, coletam dados de geolocalização por diferentes meios e diversos sistemas de comunicação, como redes *wi-fi*, sinais de GPS e *bluetooth*. A localização pode vir de sinais em tempo real, como um endereço IP por exemplo. Endereços de Protocolo de Internet (IP, na sigla em inglês) fazem parte da infraestrutura da Internet e são atribuídos a um dispositivo sempre que ele fica *on-line*. Como são baseados em geografia, podem ser usados para estimar a localização de um dispositivo. Alguns aparelhos celulares também têm um número específico, a exemplo dos que utilizam sistema *Android*. Quando o usuário acessa um site ou um aplicativo, permite que seja revelada sua localização atual. A atividade na web também pode fornecer a localização de uma pessoa. Quando, por exemplo, utiliza um motor de busca ou um serviço de e-mail, suas pesquisas e atividades podem incluir informações de localização.

Os dados de localização, captados em tempo real ou armazenados pelas operadoras de telefonia móvel e provedores de serviços na Internet, não podem ser compartilhados com outras empresas e nem com o Poder Público, a não ser em situações expressamente previstas em lei e quase sempre mediante prévia autorização judicial⁸.

Essas informações (dados de localização) são coletadas pelas operadoras de telefonia e provedores de

⁸ Sobre requisição judicial de dados armazenados por provedores de Internet, sugiro a leitura de nosso artigo intitulado "LIMITES E REQUISITOS DA ORDEM JUDICIAL PARA QUEBRA DE SIGILO DE DADOS ARMAZENADOS POR PROVEDOR DE SERVIÇOS NA INTERNET - Desnecessidade de individualização prévia do(s) investigado(s) e do esgotamento de outros meios de prova", publicado no site *Jus Navigandi*, em 03.2020, acessível em: <https://jus.com.br/artigos/80222/limites-e-requisitos-da-ordem-judicial-para-quebra-de-sigilo-de-dados-armazenados-por-provedor-de-servicos-na-internet>

serviços na Internet para o desempenho de suas atividades. Elas apenas guardam e processam as informações dos usuários de seus serviços para o desenvolvimento de atividades legítimas⁹, quando autorizadas pela lei ou mediante consentimento do titular dos dados. O fato de processar informações de terceiros, não torna a empresa titular dos dados coletados. O operador ou controlador de um sistema (informatizado ou não) que realiza o tratamento de dados pessoais não adquire a titularidade desses dados e nem tem o controle absoluto sobre eles. A guarda ou utilização dos dados é realizada apenas para atingir a finalidade da operação e pelo tempo necessário para se alcançar o objetivo pretendido. O titular continua sendo a pessoa natural a quem se referem os dados pessoais objeto do tratamento.

Assim, se o processamento dos dados foi autorizado apenas para uma finalidade específica, não podem ser utilizados para objetivos diversos. Se a operadora de telefonia e o provedor obtiveram o consentimento dos usuários para o tratamento de seus dados pessoais em uma atividade determinada, não podem utilizá-los para outros propósitos, e muito menos compartilhá-los com terceiros para serem utilizados em finalidades estranhas à informada ao titular dos dados no momento em que o consentimento foi solicitado. O provedor que necessitar comunicar ou compartilhar dados pessoais com terceiros deverá obter consentimento específico do titular dos dados para esse fim.

⁹ O ordenamento jurídico brasileiro obriga empresas do setor de telecomunicações e provedores de conexão e serviços na Internet a guardarem metadados e os dados pessoais que recolhem nas atividades prestadas a seus usuários. Esse dever legal está previsto no art. 13-B, § 4º., do CPP (na redação dada pela Lei n. 13.344/16), Lei n. 12.850/13 ("Lei das Organizações Criminosas"), Lei n. 12.965 de 2014 ("Marco Civil da Internet") e Resoluções nº 426 de 2005, 477 de 2007 e 614 de 2013 da Agência Nacional de Telecomunicações (ANATEL).

O princípio da finalidade, um dos que caracterizam o tratamento de dados legítimo, foi incorporado ao nosso ordenamento jurídico pelo art. 7º., inc. VIII, alíneas a a c, da Lei n. 12.965/14 (“Marco Civil da Internet”). A LGPD (Lei n. 13.709/18) também consagra o princípio da finalidade como uma das condições para a licitude da atividade de tratamento de dados (art. 6º., I). Embora a LGPD só entre em vigor no mês de agosto próximo, seus preceitos já servem como baliza norteadora da legitimidade de qualquer atividade que implique na utilização de dados pessoais.

O compartilhamento de dados de geolocalização, ainda que para execução de políticas públicas de combate ao coronavírus, não encontra respaldo em nossa legislação, já que não há previsão em leis e regulamentos específicos. Um compartilhamento massivo, representando pela entrega aos agentes públicos de dados de centenas de milhares de pessoas, necessitaria da edição de lei ou ato normativo específico, estabelecendo certas garantias e salvaguardas para os titulares dos dados, como a de que a utilização deve ser feita somente para a finalidade de monitorar e conter a expansão da epidemia do coronavírus, a determinação de um prazo para a atividade de tratamento, medidas de segurança para a guarda dos dados e a previsão de eliminação das informações quando encerrado o estado de emergência, dentre outras medidas.

A Lei 13.979/2020, que prevê medidas para enfrentamento da emergência de saúde pública de importância internacional decorrente do coronavírus, não elenca, dentre elas, a utilização de dados de geolocalização em poder das companhias de telefonia e provedores de Internet. Assim, seria necessária a edição de uma nova lei ou medida provisória, estabelecendo a

abrangência, limites e garantias aos indivíduos para o compartilhamento de dados pessoais. No nível estadual e municipal, talvez fosse possível a edição de decretos pelos governadores e prefeitos, definindo a forma e amplitude da utilização dos dados na execução da política de combate ao coronavírus. As normas teriam que definir, para o compartilhamento de dados, limites temporais e espaciais indispensáveis à promoção e preservação da saúde pública.

Sem essa regulamentação, é quase certo que qualquer iniciativa de criar sistemas de monitoramento e controle massivo dos cidadãos brasileiros, por meio de smartphones e geolocalização, seja barrada nos tribunais. Ainda que em situação de emergência ou de interesse humanitário, a coleta de dados em massa tem que ter previsão legal, definindo seus contornos e estabelecendo limitações. A vigilância em massa não tem respaldo hoje e certamente seria declarada inconstitucional medida governamental destinada a implantá-la sem qualquer limite, porque fere princípios fundamentais de nossa Constituição. Não apenas o preceito que garante a inviolabilidade da vida privada e privacidade individual (art. 5º., X) poderia restar violado, mas também o garante a liberdade de locomoção (art. 5º., XV).

É imprescindível que os chefes do Poder Executivo, nas diversas esferas onde está ocorrendo a implantação das medidas públicas de contenção e controle do vírus, tomem a iniciativa de regulamentar imediatamente a recolha e o tratamento dos dados de geolocalização, indicando expressamente, na norma regulamentar (que pode ser uma medida provisória, um decreto etc.), as garantias precisas quanto ao objetivo, escopo de aplicação, modalidade, duração e segurança dos dados. Essa regulamentação poderia vir na forma de uma

Portaria de um Ministro de Estado ou norma de uma agência reguladora, como a Anatel por exemplo. Sem uma intervenção regulatória, o uso de sistemas massivos de vigilância não se legitima. Apesar da emergência em andamento, políticas públicas de contenção e controle do vírus baseadas no uso indiscriminado e massivo de dados de geolocalização necessitam de regulamentação apropriada.

Mesmo sobrevivendo normas regulamentadoras (quer na forma de medida provisória, decreto, regulamento ou mesmo lei em sentido formal), ainda poderiam ser invalidadas nos tribunais. As regras iriam estar sujeitas posteriormente ao controle da constitucionalidade, especificamente para análise da proporcionalidade das medidas. Caberia provavelmente ao STF dar a última palavra quanto ao uso dos sistemas de vigilância massivos. A corte constitucional certamente seria chamada para avaliar se, diante da situação emergencial da epidemia do coronavírus, o compartilhamento e utilização de dados de geolocalização seria justificado ou desproporcional, se causar reflexos mais danosos à privacidade individual. Ao tribunal caberia examinar, em cada caso, se o compartilhamento não estaria sendo feito de forma excessiva ou mais invasiva que o necessário para possibilitar o combate à epidemia. A indicação de certos limites e garantias na norma regulamentadora, para a recolha e uso dos dados, são elementos que serviriam como parâmetros indicativos da proporcionalidade da medida.

Nas notícias que se seguiram quanto à implantação de sistemas de controle da epidemia, os responsáveis pelos projetos de monitoramento do movimento das pessoas, com base em dados de geolocalização, foram categóricos em afirmar que só são utilizados "dados agregados", que não permitem a identificação das pessoas.

Se os dados que estão sendo compartilhados e utilizados nesses projetos de acompanhamento da evolução da pandemia não permitem identificar as pessoas, então a preocupação com a privacidade deixa de ser elemento a ser considerado. Realmente, alguns registros de localização e dados em poder das operadoras de telefonia e provedores vinculam-se diretamente aos dispositivos (aparelhos celulares), exclusivamente, e não aos titulares dos equipamentos móveis. Se não se trata de dados pessoais, assim considerados os que se relacionam a uma pessoa natural identificada ou identificável, desaparece o risco de invasão à privacidade alheia. Da mesma forma, se os dados pessoais, antes de compartilhados, estão sendo objeto de algum processo eficaz de "anonimização", impedindo que os titulares possam ser identificados, também não há razão para preocupação.

O **Comitê Europeu de Proteção de Dados** (CEPD)¹⁰ publicou recentemente uma espécie de "guidelines", para orientar os países membros quanto à questão da utilização de dados de geolocalização em iniciativas de combate ao coronavírus. Lembrando que as leis de proteção de dados não se aplicam a dados que tenham sido apropriadamente anonimizados, o CEPD orienta os Estados europeus a se limitar ao uso de dados de localização de maneira a não identificar indivíduos:

"As autoridades públicas devem primeiro buscar processar dados de localização de

¹⁰ O Comitê Europeu para a Proteção de Dados (CEPD) é um organismo europeu independente que contribui para a aplicação coerente de regras em matéria de proteção de dados na União Europeia e promove a cooperação entre as autoridades de proteção de dados da UE. O CEPD é composto por representantes das autoridades nacionais para a proteção de dados e a Autoridade Europeia para a Proteção de Dados (AEPD). Ver maiores informações no site oficial do CEPD, acessível em: https://edpb.europa.eu/about-edpb/about-edpb_pt

uma maneira anônima (p.ex., processando dados agregados de uma maneira que os indivíduos não possam ser reidentificados), que podem proporcionar a geração de relatórios de concentração de dispositivos móveis numa certa localidade ("cartografia")¹¹.

Somente se não for possível o uso de dados anonimizados, é que o CEPD sugere, então, a adoção de medidas regulatórias, para garantir a proporcionalidade das políticas de vigilância social¹².

A preocupação aqui no Brasil é que ainda não foi implantada a Agência Nacional de Proteção de dados - ANPD (prevista no art. 55-A da LGPD). Sem uma agência reguladora para proteção de dados não se tem como acompanhar e fiscalizar os projetos públicos de controle de movimentação de pessoas, o que pode fragilizar a privacidade individual.

Proteção de dados não é incompatível com medidas para combater a epidemia do coronavírus. Mesmo em tempos excepcionais, as autoridades públicas não podem descuidar da preservação da privacidade dos cidadãos. É preciso garantir de que a utilização de dados de localização, ainda que de forma anônima, não represente um risco à segurança e privacidade dos indivíduos. Ninguém é contra o uso de dados pessoais para um monitoramento e

¹¹ "Public authorities should first seek to process location data in an anonymous way (ie. processing data aggregated in a way that individuals cannot be re-identified), which could enable generating reports on the concentration of mobile devices at a certain location ("cartography")."

¹² As *guidelines* para equilibrar proteção de dados com as políticas públicas de combate ao coronavírus estão disponíveis no seguinte endereço:

https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_2020_processingpersonaldataandcovid-19_en.pdf

controle da expansão da epidemia, desde que isso resulte na preservação da vida humana. Entretanto, nenhuma pessoa gostaria de ver seus dados pessoais usados pelo Governo para propósitos que se desviassem do interesse público.

Recife, 27.03.20