# O GOVERNO BRASILEIRO VIOLA O DIREITO À PRIVACIDADE AO OBTER DADOS DE LOCALIZAÇÃO ATRAVÉS DO CORONAVÍRUS - SUS?

*Ester Dutra Pereira*[1]

*Karine Lopes da Cruz Sousa*[2]

O Coronavírus – SUS é um aplicativo desenvolvido pelo Departamento de Informática do SUS (DataSus) com o objetivo de conscientizar a população sobre o COVID-19, informar sobre os possíveis sintomas, maneiras de se prevenir e o que fazer em caso de suspeita de infecção, além de indicar as unidades de saúde mais próximas dos usuários. Segundo o Ministério da Saúde (BRASIL, 2020), o *app*, que está disponível de forma gratuita para Android e iOS desde 28 de fevereiro de 2020, foi baixado por mais de 3,5 milhões de usuários e, a princípio, é uma importante estratégia do Governo Federal no combate à COVID-19 no país.

Ao fazer o *download* do Coronavírus - SUS nas lojas virtuais, verifica-se que o aplicativo poderá solicitar acesso à localização do dispositivo, ligações diretas para números de telefone, leitura de notificação do dispositivo e outras funcionalidades ligadas à rede móvel. Não é exigido cadastro para que o usuário navegue na aba de notícias e dicas, mas, para realizar uma autoavaliação clínica, são solicitadas informações como idade, sexo e sintomas e, para ter acesso às unidades de saúde próximas ao dispositivo, o aplicativo solicita geolocalização.

Não é apenas no Brasil que esse tipo de política pública apoiada na tecnologia está sendo implementado. Diversos países têm investido em ferramentas tecnológicas de geolocalização para *contact tracing*[3], permitindo que as autoridades direcionem recursos, garantam o isolamento social e controlem a transmissão do vírus.

A geolocalização é um recurso que, por meio da coleta de informações de um celular, registra os locais em que a pessoa esteve. No contexto da pandemia, a geolocalização tem sido relevante para alguns países, pois permite monitorar a movimentação das pessoas, de forma a garantir o cumprimento do isolamento social, recomendação anunciada pelas autoridades de saúde como medida de enfrentamento ao vírus. Todavia, há que se questionar a possibilidade de tal monitoramento interferir no direito à privacidade e à liberdade dos cidadãos.

---

[1] Graduanda em Direito na Universidade Federal do Rio de Janeiro. E-mail: esterpdutra@gmail.com.

[2] Graduanda em Direito na Universidade Federal do Rio de Janeiro, integrante do Núcleo de Pesquisa sobre Proteção de Dados da Liga de Direito e Tecnologia da UFRJ e membro da Empresa Júnior Destro Consultoria Jurídica. E-mail: karinelopes3@gmail.com.

[3] *Contact tracing* (rastreamento de contato) visa identificar pessoas contaminadas pelo Coronavírus, detectando e informando os que tiveram contato com elas, a fim de evitar a propagação do vírus. O rastreamento pode ser feito por GPS, *wi-fi* ou *bluetooth*.

Dado que o aplicativo Coronavírus - SUS acessa os dados de geolocalização dos usuários, surge uma série de preocupações. A coleta e a utilização dos dados são autorizadas? É feita a anonimização? Qual é o destino dessas informações individuais? O que acontecerá com os dados coletados após o atual estado de emergência? Há violação da proteção de dados e da privacidade? Assim, é relevante analisar o aplicativo e sua conformidade com a legislação.

No Brasil, as principais legislações sobre as condições e limites da coleta de dados são a Lei n° 13.979/20[4] e a Lei Geral de Proteção de Dados Pessoais (LGPD - Lei nº 13.709/2018), que ainda não está em vigor.

Na Lei n° 13.979/20, o art. 6°, único que versa sobre o compartilhamento de dados pessoais de infectados, ou com suspeita de infecção, entre entes públicos, "com a finalidade exclusiva de evitar a sua propagação", não dispõe sobre o tratamento dos dados, não leva em consideração o direito do titular de acompanhar o uso de suas informações, não define quais os tipos de dados poderão ser compartilhados e não especifica qual será o tratamento oferecido aos dados pessoais após o término da pandemia e da vigência da Lei, que é temporária.

Em relação à LGPD, é possível interpretar o tratamento de dados geolocacionais conforme os princípios contidos no Art. 6°[5]. Se o aplicativo coletar a localização do usuário solicitando o seu consentimento, especificando a finalidade do tratamento e garantindo a segurança e anonimização dos dados, não há violação aos direitos do titular.

Na tentativa de verificar o cumprimento dos parâmetros legislativos acima pelo aplicativo Coronavírus - SUS, analisamos seus Termos Legais de Uso, que estabelecem que os órgãos de pesquisa poderão acessar a base de dados pessoais dos utilizadores na realização de estudos, sendo garantido o tratamento exclusivamente dentro dos órgãos e para a finalidade da pesquisa. Em princípio, há a garantia do sigilo e do anonimato e, em nenhuma circunstância, é permitida a transferência de dados a terceiros. Todavia, segundo uma pesquisa do Internet Lab, o Lumem, ferramenta que identifica riscos em aplicativos, detectou tráfego de dados para a empresa Dynatrace (GOMES et al, 2020).

Isso leva à possibilidade do tratamento dos dados pessoais pelo aplicativo não ser transparente, deixando dúvidas sobre qual seria o objetivo de sua coleta, qual será sua destinação, além de receios quanto à possibilidade de reversão da anonimização.

---

[4] Dispõe sobre as medidas para enfrentamento da emergência de saúde pública de importância internacional decorrente do coronavírus responsável pelo surto de 2019.

[5] São estes: boa-fé, finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização e prestação de contas.

Em tese, poder-se-ia recorrer às citadas bases legislativas, contudo, a generalidade do art. 6° da Lei 13.979/2020 também parece implicar na sua impossibilidade de garantir o direito à privacidade, motivo pelo qual o dispositivo precisa ser aplicado levando em consideração o ordenamento jurídico. É crucial que os cidadãos brasileiros conheçam os métodos de vigilância de dados aplicados nos aplicativos, sob pena de que os aparelhos celulares venham a concretizar as funções das teletelas da distopia 1984, de George Orwell.

Essa problemática pode apontar para uma suposta dicotomia entre privacidade e segurança que, considerando a gravidade do atual cenário mundial, terminaria por flexibilizar a primeira. Essa oposição, contudo, é falsa, pois privacidade e segurança são direitos complementares assegurados pela Constituição. A administração pública pode, e deve, promover a segurança coletiva sem afetar a proteção dos dados e da privacidade da população.

Exemplo prático dessa complementaridade é o aplicativo Trace Together, lançado pelo governo de Singapura como estratégia de combate ao vírus. Utilizando a tecnologia *bluetooth*, o programa rastreia os contatos digitais dos usuários, mas há compartilhamento de dados somente entre telefones próximos e apenas se o usuário testar positivo para o COVID-19. Os dados são armazenados por 25 dias nos próprios aparelhos e automaticamente excluídos após o prazo. A localização não é monitorada em tempo real, os dados pessoais, tais como nome e endereço e a lista de contatos não são coletados e o aplicativo não utiliza dados de localização por GPS ou *wi-fi*. (TRACE TOGETHER, 2020).

Seria interessante que os entes públicos brasileiros desenvolvessem ferramentas de *contact tracing* com a utilização de *bluetooth* em vez de dados de geolocalização, a fim de não identificar as pessoas e proteger a privacidade dos usuários, tal como determina o ordenamento jurídico. Contudo, o que existe no Brasil atualmente é o contrário disso: todos os dados são coletados, mas não há rastreamento de contatos efetivo na prevenção e combate ao contágio.

A tecnologia é uma interessante estratégia para o controle de contaminação do COVID-19, mas não é eficaz sem quantidade de testes suficiente e insumos básicos para enfrentar a atual situação. Ademais, é urgente a entrada em vigor da LGPD e a concretização da Autoridade Nacional de Proteção de Dados (ANPD)[6], que devem ser levadas a sério para garantir a efetivação de direitos fundamentais previstos na Constituição Federal.

[6] A LGPD criou a ANPD e lhe atribuiu a competência para regulamentar assuntos específicos não tratados por ela, mas o órgão ainda não é operacional. Diretrizes normativas sobre o tratamento de dados de localização seriam essenciais para garantir suas devidas finalidades e, ao mesmo tempo, o direito à privacidade, sobretudo em estados de emergência, tais como a pandemia do COVID-19.

**REFERÊNCIAS**


BIONI, Bruno R. *et al*. **Os dados e o vírus: pandemia, proteção de dados e democracia** [Livro eletrônico] – São Paulo: Reticências Creative Design Studio, 2020.

BRASIL. **Lei 13.979, de 6 de fev. de 2020.** Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/l13979.htm. Acesso em: 28 jul. 2020.

BRASIL. **Lei Geral de Proteção de Dados Pessoais (LGPD).** Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 27 jul. 2020.

BRASIL. Ministério da Saúde. **Aplicativo Coronavírus SUS agora envia mensagens de alertas aos usuários.** Disponível em: https://www.saude.gov.br/noticias/agencia-saude/46628-aplicativo-coronavirus-sus-agora-envia-mensagens-de-alertas-aos-usuarios. Acesso em: 29 jul. 2020.

GOMES, Alessandra *et al*. **COVID-19: Apps do governo e seus riscos à privacidade.** Disponível em: https://www.internetlab.org.br/pt/privacidade-e-vigilancia/covid-19-apps-do-governo-e-seus-riscos/. Acesso em: 25 jul. 2020.

TRACE TOGETHER. Disponível em: https://www.tracetogether.gov.sg. Acesso em: 29 jul. 2020.