ANAJURE – Associação Nacional de Juristas Evangélicos

www.anajure.org.br

"Em Defesa das Liberdades Civis Fundamentais"

NOTA PÚBLICA
UTILIZAÇÃO DE DADOS DE GEOLOCALIZAÇÃO COMO MEDIDA DE COMBATE À PANDEMIA DO CORONAVÍRUS

O **Conselho Diretivo Nacional da Associação Nacional de Juristas Evangélicos – ANAJURE**, no uso das suas atribuições estatutárias e regimentais, emite à sociedade brasileira a presente Nota Pública, sobre a utilização de dados de geolocalização como medida de combate à pandemia do coronavírus.

I – SÍNTESE FÁTICA

Nos últimos dias, noticiou-se que as operadoras de telefonia móvel, em parceria, fornecerão ao Ministério da Ciência, Tecnologia, Inovações e Comunicações (MCTIC) dados de mobilidade que permitem monitorar deslocamentos e pontos de ajuntamento da população, como forma de auxiliar no combate à proliferação da COVID-19.

Sobre isso, o Sindicato Nacional das Empresas de Telefonia e de Serviço Móvel Celular e Pessoal – SINDITELEBRASIL informou que os dados estarão em nuvem pública (*data lake*) e serão organizados de forma agregada e anônima, de acordo com as normas da Lei Geral de Proteção de Dados (LGPD) e do Marco Civil da Internet[1].

Medidas semelhantes vêm sendo adotadas em alguns países. Na Coréia do Sul, estão sendo utilizadas imagens de câmeras de vigilância, dados de localização de smartphones e registros de compras de cartão de crédito para rastrear o deslocamento de pacientes com coronavírus e estabelecer a cadeia de transmissão do vírus. Na Lombardia, Itália, as autoridades estão se valendo dos dados transmitidos pelos celulares

[1] https://www.sinditelebrasil.org.br/sala-de-imprensa/releases/3375-operadoras-vao-disponilizar-dados-de-mobilidade-ao-mctic-para-monitorar-deslocamento

para aferir a quantidade de pessoas em isolamento e as distâncias que os cidadãos têm percorrido. Em Israel, por meio de um mecanismo antes utilizado para operações de contraterrorismo, o governo pretende monitorar dados de localização dos celulares para identificar pessoas que possam ter sido expostas ao coronavírus[2].

No Brasil, o MCTIC ensaiou uma utilização de dados de geolocalização, mas recuou após orientação do Presidente da República, que determinou o adiamento da iniciativa até que outras análises sejam efetuadas pelo Governo. Em alguns estados brasileiros, no entanto, a ação já está em prática. A respeito disso o Min. Marcos Pontes (MCTIC), manifestou-se afirmando que os estados têm autonomia para firmar acordos com as operadoras[3].

O assunto é bastante controverso e tem suscitado debates mundo afora, visto que levanta temores referentes à proteção de dados e à privacidade.

II – CONSIDERAÇÕES SOBRE PRIVACIDADE E PROTEÇÃO DE DADOS

II.I – Disposições da legislação brasileira sobre a proteção da privacidade e dos dados

A Constituição Federal de 1988 resguarda, no rol dos direitos fundamentais, a intimidade, a vida privada, a honra e a imagem das pessoas (art. 5°, inciso X, CF/88), bem como estabelece que é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal (art. 5°, inciso XII, CF/88).

O Código de Defesa do Consumidor (Lei n. 8.078/1990) estabelece que "a abertura de cadastro, ficha, registro e dados pessoais de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele" (art. 43, § 2°).

O Marco Civil da Internet (Lei n. 12.965/2014) prevê como princípio do uso da internet no Brasil a proteção da privacidade, a proteção dos dados pessoais, na forma da lei e a responsabilização dos agentes de acordo com suas atividades, nos termos da lei (incisos II, III e VI, do art. 3°, da Lei n. 12.965/2014). Outros direitos são assegurados pelo Marco Civil da Internet ***(art. 7°)***: inviolabilidade da intimidade e da vida privada, havendo indenização em caso de violação ***(inciso I)***; não fornecimento a terceiros de

[2] https://www.nytimes.com/2020/03/23/technology/coronavirus-surveillance-tracking-privacy.html
[3] https://g1.globo.com/politica/noticia/2020/04/13/governo-adia-uso-dados-de-celulares-para-monitorar-deslocamento-das-pessoas.ghtml

seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei ***(inciso VII)***; informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidade que ***a)*** justifiquem sua coleta, ***b)*** não sejam vedadas pela legislação, e ***c)*** estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet ***(inciso VIII)***; consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais ***(inciso IX)***.

O MCI ainda dispõe que "a guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, ***devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas***" (art. 10°).

Especificamente para o contexto de combate da COVID-19, a Lei 13.979/2020, dispôs que é obrigatório o compartilhamento entre órgãos e entidades da administração pública federal, estadual, distrital e municipal de dados essenciais à identificação de pessoas infectadas ou com suspeita de infecção pelo coronavírus, com a finalidade exclusiva de evitar a sua propagação (art. 6°, Lei 13.979/2020). A imposição é estendida às pessoas jurídica de direito privado quando houver solicitação da autoridade sanitária (art. 6°, § 1°, Lei 13.979/2020).

No Brasil, ainda temos a Lei Geral de Proteção de Dados (Lei n. 13.709), de14 de agosto de 2018, com entrada em vigor programada, inicialmente, para 18 meses após sua publicação oficial, prazo que foi alterado para 24 meses pela Medida Provisória n. 869/2018, convertida na Lei 13.853/2019.

A LGPD também tem como fundamentos o respeito à privacidade e a inviolabilidade da intimidade, da honra e da imagem (incisos I e IV, do art. 2°). Segundo o **art. 7°** da referida lei, o tratamento de dados pessoais somente poderá ser realizado, dentre outras exigências, mediante o fornecimento de consentimento pelo titular ***(inciso I)***; para o cumprimento de obrigação legal ou regulatória pelo controlador ***(inciso II)***; pela administração pública, com fins de políticas públicas previstas em leis, regulamentos, contratos, convênios ou instrumentos congêneres ***(inciso III)***; para a proteção da vida ou da incolumidade física do titular ou de terceiro ***(inciso VII)***; para a tutela da saúde,

exclusivamente, em procedimento realizado por profissionais de saúde, serviço de saúde ou autoridade sanitária ***(inciso VIII)***.

Ainda há, na LGPD, disposição referente ao término do tratamento de dados pessoais, na qual se estabelece que:

> Art. 15. O término do tratamento de dados pessoais ocorrerá nas seguintes hipóteses:
> I - verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada;
> II - fim do período de tratamento;
> III - comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento conforme disposto no § 5º do art. 8º desta Lei, resguardado o interesse público; ou
> IV - determinação da autoridade nacional, quando houver violação ao disposto nesta Lei.

Dentre os direitos da pessoa natural ***(art. 18)***, há a possibilidade de requisição de anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na Lei ***(inciso IV)***; a eliminação dos dados pessoais tratados com o consentimento do titular, ressalvadas exceções legais[4] ***(inciso VI)***; informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa ***(inciso VIII)***; e a revogação do consentimento ***(inciso IX)***.

Ademais, a LGPD contém previsões referentes às sanções administrativas cabíveis em casos de infrações às normas por ela previstas, fixando possibilidade de aplicação de advertência, multas, eliminação de dados pessoais, dentre outras (art. 52 da lei mencionada).

No entanto, conforme já exposto, a LGPD ainda não está em vigor e este contexto coloca a população brasileira em situação de vulnerabilidade no tocante à proteção de dados e à privacidade.

II.II – Terminologia aplicável ao compartilhamento de dados

[4] LGPD: Art. 16. Os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades:
I - cumprimento de obrigação legal ou regulatória pelo controlador;
II - estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
III - transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou
IV - uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.

Alguns termos não são usuais, seja no âmbito jurídico, seja no cotidiano das pessoas, de modo que pode ser útil esclarecê-los antes de tecer outras considerações.

> **DADO ANONIMIZADO**: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento (art. 5°, III, LGPD).
>
> **ANONIMIZAÇÃO:** utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo (art. 5°, XI, LGPD).
>
> **DADOS AGREGADOS:** dados resumidos ou tratados estatisticamente[5]. São dados apresentados de modo compilado, e não individualmente[6].
>
> **DADOS DESAGREGADOS:** dados que não foram processados estatisticamente e estão disponíveis sob a forma em que foram adquiridos[7].

II.III – Proteção dos dados e da privacidade no contexto de pandemia

Em que pese a LGPD não tenha entrado em vigor, a CF/88, o CDC e o MCI fornecem princípios e disposições que podem nortear o tratamento de dados, sendo necessário frisar e adotar como elementos norteadores deste debate a proteção da privacidade, da intimidade, da honra e da imagem das pessoas. Das normas acima, podemos extrair uma consonância referente à valorização da transparência, da privacidade e da manifestação expressa de consentimento no tocante ao fornecimento de dados.

Nesse sentido, especialistas e instituições comprometidas com a defesa das liberdades civis fundamentais e com a privacidade têm se posicionado e proferido alertas a respeito da utilização de dados de geolocalização.

Um dos pontos para o qual se tem dado destaque é existência de técnicas capazes de reverter a anonimização gerada por dados agregados, ainda que não existam

---

[5] https://www.survio.com/br/pesquisa-terminologia.
[6] https://link.estadao.com.br/noticias/cultura-digital,uso-de-dados-de-localizacao-no-combate-a-covid-19-pode-ameacar-privacidade,70003268063
[7] Ibid.

informações específicas, como nome e endereço, no pacote de dados[8]. Nessas hipóteses, seria possível ocorrer a reidentificação do sujeito. Quanto a isso, a Electronic Frontier Foundation – EFF (Fundação Fronteira Eletrônica) explicou que:

> Há uma diferença entre dados de localização "agregados" e dados de localização "anonimizados" ou "não-identificados". Na prática, no entanto, não é possível remover a identificação de dados individuais de localização. Normalmente, informações sobre onde uma pessoa está ou onde já esteve são suficientes para que ocorra a reidentificação. Alguém que se desloca frequentemente entre um escritório e uma casa compartilhada por apenas uma família é provavelmente a única pessoa a manter esse hábito e, portanto, identificável por meio de outras fontes prontamente identificáveis. Um estudo de 2013 amplamente citado descobriu que pesquisadores conseguem identificar 50% das pessoas utilizando apenas dois dados de tempo e de localização escolhidos aleatoriamente[9].

Por isso, uma das recomendações feitas pela EFF é de que ***dados de localização "não-identificados" e "anonimizados" que não são agregados sejam evitados***. Outra consideração feita pela EFF diz respeito à eficácia do uso de dados extraídos das redes móveis. Segundo a instituição, algumas limitações devem ser consideradas pelas autoridades que pretendem chegar a conclusões a partir desses dados, como o fato de que parte da população não possui acesso a smartphones. Por isso, os governos correm o risco de tomar decisões que ignoram as necessidades e o contexto de pessoas com poucos recursos e que já são marginalizadas. Ilustrando a situação, a EFF menciona o caso de indivíduos que se deslocam mais, não por insubmissão ante a recomendação de isolamento, e sim por percorrerem distâncias maiores para ter acesso a serviços essenciais.

Na conjuntura brasileira, temos uma situação particular em que não há legislação em vigor apta a estabelecer de forma clara a limitação do tratamento de dados e, ainda que estabeleça algumas restrições, não detalha as sanções possíveis para desestimular e coibir os excessos. Assim, temos um cenário que pode resultar em riscos à segurança jurídica.

II.IV - Recomendações relativas à utilização de dados e à proteção da privacidade

[8] https://link.estadao.com.br/noticias/cultura-digital,uso-de-dados-de-localizacao-no-combate-a-covid-19-pode-ameacar-privacidade,70003268063
[9] https://www.eff.org/pt-br/deeplinks/2020/04/how-protect-privacy-when-aggregating-location-data-fight-covid-19

Diante dos elementos expostos até este ponto, entendemos que a utilização de dados fornecidos pelas operadoras de telefonia móvel, no Brasil, carece de balizas legais aptas a protegerem a privacidade das pessoas, devendo ser evitada. Considerando, no entanto, que alguns estados já têm feito uso de tais mecanismos compreendemos ser necessário dispor algumas recomendações que possam minimizar os efeitos colaterais do monitoramento de dados de geolocalização, na linha do que tem sido proposto por organizações comprometidas com a proteção da privacidade espalhadas pelo mundo[10]. Vejamos:

LEGALIDADE

1. Em nome do princípio da legalidade, eventuais restrições à privacidade devem ser previstas expressamente pela legislação nacional, a qual deverá estabelecer limites e sanções ao tratamento de dados.

PROPORCIONALIDADE

2. O eventual uso de dados dos cidadãos deve ser proporcional à necessidade existente e fundamentado em objetivos relacionados à saúde pública.

TRANSPARÊNCIA

3. A metodologia de coleta e tratamento de dados deve ser divulgada, além de se expor com quem tais informações são compartilhadas e com qual finalidade.

CONSENTIMENTO

4. É necessário que as pessoas estejam a par das implicações do monitoramento de dados e, informadas, possam expressar seu consentimento ou sua recusa a respeito do referido uso.

---

[10] As recomendações listadas foram organizadas com base em orientações expedidas pela EFW e por uma série de instituições com atuação na área dos direitos humanos que publicaram uma nota intitulada "Declaração conjunta da Sociedade Civil: A utilização das tecnologias de vigilância digital pelos Estados para combater a pandemia deve respeitar os direitos humanos". EFF: https://www.eff.org/pt-br/deeplinks/2020/04/how-protect-privacy-when-aggregating-location-data-fight-covid-19
Declaração conjunta da Sociedade Civil: https://www.hrw.org/news/2020/04/02/joint-civil-society-statement-states-use-digital-surveillance-technologies-fight

5. Quanto a isso, também é necessário que se assegure às pessoas a possibilidade de revogar o seu consentimento e de pedir a exclusão dos seus dados.

FINALIDADE DO USO

6. A eventual utilização de dados agregados de localização das pessoas deve estar atrelada unicamente à tomada de medidas de saúde pública, servindo como norte para adoção de melhores estratégias ao combate da COVID-19. Assim, estão excluídos, por exemplo, o uso com fins punitivos e com objetivos comerciais.

NÃO-IDENTIFICAÇÃO

7. Evitar procedimentos de reidentificação de pessoas cujos dados foram colhidos em alguma espécie de monitoramento.

MONITORAMENTO TEMPORÁRIO

8. Eventuais monitoramentos executados devem ter delimitação temporal, relacionada neste caso aos picos da COVID-19, não sendo possível que permaneçam em curso indefinidamente. Encerrada a necessidade, a utilização de dados deve ser cessada e estes devem ser excluídos.

III - CONCLUSÃO

Ex Positis, a ANAJURE **(i)** alerta a respeito dos riscos decorrentes do uso de dados de geolocalização, no contexto da pandemia, para o direito fundamental à privacidade; **(ii)** sustenta que qualquer medida de compartilhamento de dados deve vir acompanhada da devida regulamentação legal, não existindo, atualmente, uma norma desse caráter em vigor no Brasil; **(iii)** qualquer medida, bem como qualquer legislação sobre tratamento de dados, devem atender aos critérios da legalidade, proporcionalidade, transparência, consentimento, delimitação da finalidade, não-identificação e temporariedade.

Brasília, 14 de abril de 2020.

Dr. Uziel Santana
Presidente da ANAJURE

Dr. Felipe Augusto Carvalho
Diretor Executivo da ANAJURE