Consultor Jurídico
conjur.com.br

DIREITO DIGITAL

Dados de geolocalização e a investigação do caso Marielle

7 de julho de 2020, 16h02

Por Juliana Abrusio, Juliano Maranhão, Ricardo Campos e Nuria López

O historiador de tecnologia americano Michael S. Mahoney expressou de forma clara a mudança que afeta a sociedade atual: na sua opinião, não há duplicidade de mundos, ou seja, por um lado o mundo analógico e real e, por outro, o mundo digital e virtual, mas há uma transferência do mundo offline, analógico para o computador e as suas redes[1]. A utilização em larga escala pela população de aparelhos e máquinas interligadas entre si em redes computacionais traz consigo novas chances, mas traz também novos perigos às sociedades liberais modernas.

Atualmente, por meio dos dispositivos móveis, deixamos rastros digitais por onde andamos, incluindo dados de "geolocalização", muitas vezes considerados sensíveis por proporcionar um panorama esmiuçado sobre os deslocamentos físicos de uma pessoa, com a possibilidade de inferir hábitos, relacionamentos, preferências e diversas outras ilações[2]. Nesse quadro, talvez se possa até dizer que não há mais mundo off-line. O tratamento inadequado desses dados pessoais pode resultar em situações abusivas e ilegais, com repercussões que violam as garantias individuais.

A análise de dados (*data analytics*) tem se mostrado eficaz em diversas atividades relacionadas à investigações criminais, como identificar o local do crime, o criminoso, monitorar um suspeito ou um padrão de comportamento criminoso, e com efetividade em casos de pessoas desaparecidas ou sequestradas[3], de modo que a tecnologia deve ser usada para elevar a eficiência e acurácia das investigações. Porém, a circulação de dados pessoais entre as autoridades competentes para tais efeitos, incluindo a manutenção da segurança pública, deve respeitar as liberdades individuais.

Há, hoje, vozes utilitaristas no direito penal, que remontam ao ideal iluminista de Beccaria[4] do século 18 e não tem peias até mesmo diante da concretização tecnológica do panóptico Bentham. Mas a disponibilidade da tecnologia não autoriza seu uso indiscriminado pelas autoridades, sem antes passar pelo filtro dos direitos fundamentais.

Essa questão será enfrentada, em breve, pela 3ª Seção do Superior Tribunal de Justiça, que decidirá sobre a quebra de sigilo telemático de dispositivos determinados por geolocalização, para contribuir na investigação do caso da vereadora carioca Marielle Franco e do seu motorista Anderson Gomes, assassinados em março de 2018, no Rio de Janeiro. Segundo o relator do caso, o ministro Rogerio Schietti Cruz, o tema é de extrema relevância *"notadamente diante do aparente confronto entre o direito à privacidade dos indivíduos e o interesse público na atividade de persecução penal e de segurança pública"*[5].

O Ministério Público do Rio de Janeiro pretende obter dados de geolocalização de todos os usuários que estavam nos arredores de onde foi visto o carro usado pelos atiradores em um intervalo de quinze minutos, bem como buscas no Google de qualquer usuário que tenha procurado por determinados termos específicos ("Marielle Franco", "vereadora Marielle", "agenda Marielle", "agenda vereadora Marielle", "Casa das Pretas", "Rua dos Inválidos 122" e "Rua dos Inválidos") até cinco dias antes do crime.

Dada a amplitude da ordem mencionada, no caso Marielle, junto com os dados pessoais, inclusive dados de comunicações, dos possíveis suspeitos, o Ministério Público terá os dados de qualquer pessoa que esteve próxima da cena do crime e de qualquer pessoa que tenha pesquisado sobre alguma das referidas palavras-chave ainda que elas não tenham relação alguma com o ato criminoso. Pessoas que podem ter buscado pelo nome da vereadora por qualquer outro motivo, por ser partidário de suas ideias, por exemplo, ou ainda pessoas que estivessem nas proximidades do centro do Rio de Janeiro naquela noite. Nesse cenário amplo de investigação viola-se a privacidade de todos esses usuários, na tentativa de encontrar algum suspeito, além do grave risco de serem levados à investigação criminal em razão da geolocalização ou de buscas *online* registradas por seus dispositivos.

Para balizar a questão, vale observar a experiência internacional.

Nos Estados Unidos, havia posicionamento jurisprudencial até 2015, no sentido de *"que o usuário não tem uma razoável expectativa de privacidade sobre seus dados de geolocalização"* pois carrega seus dispositivos para todo lado e concordou com suas políticas de privacidade.

Porém, esse cenário se alterou diante da adoção da prática de *geofencing* ou *busca reversa* por agentes federais americanos, em 2016, na Carolina do Norte e que se espalhou para estados como California, Flórida, Minnesota e Washington.[6] Um caso específico chamou a atenção da imprensa americana ao cobrir, em dois mandados, uma área de 29.387 metros quadrados, equivalente a 3 hectares, em período de 9 horas, obrigando a empresa a entregar à polícia federal americana dados de 1.500 dispositivos armazenados em um banco de dados chamado Sensor Vault[7]. O tema voltou aos holofotes em casos relevantes como o *Cambridge Analytica*[8] e em marcos legais recentes o *California Consumer Privacy Act*[9].

Diante do espanto que os números de *geofencing* tem causado, inclusive em membros do Congresso Americano[10], é possível esperar julgamentos judiciais específicos revisitando o tema da expectativa de privacidade dos usuários diante da nova cultura de privacidade que tem se desenvolvido no país. Nesse sentido, a Suprema Corte decidiu, em 2018, no sentido de que é necessário mandado específico para obtenção de dados de conexão de dispositivos em estações rádio base próximas a cenas de crime por companhias de telecomunicações em *Carpenter v. Estados Unidos*[11].

Na Europa, no contexto de combate ao terrorismo, intensificado após os atentados de Londres em 2005, foi editada a Diretiva 2006/24 (Diretiva de Retenção de Dados), obrigando companhias de telecomunicações a manter, por ao menos seis meses, os registros de dados pessoais de seus usuários para sua eventual utilização em investigações. Porém, esse impulso foi contido em razão da violação indiscriminada à privacidade de todos os seus cidadãos que a Diretiva de Retenção de Dados representava[12]. Assim, em abril de 2014 a Diretiva foi invalidade pelo Tribunal de Justiça da União Europeia, com fundamento na proteção à privacidade, considerando que a investigação indiscriminada não pode prevalecer, mesmo quando objetiva combater infrações graves como o terrorismo. Ou seja, mesmo a grave ameaça representada pelo terrorismo foi insuficiente para justificar uma atuação de vigilância sobre todos os usuários de telecomunicações (*dragnet surveillance*).

Uma conjugação de utilização possível de dados de geolocalização em investigações criminais e a observância do direito à privacidade dos usuários, que em regra não terão relação com a atividade criminosa, deve passar pelo estabelecimento de critérios de proporcionalidade que impeçam a vigilância em massa[13], reduzindo a análise aos dados pessoais do investigado.

Mesmo assim, deve-se garantir a qualidade dos dados, para evitar que a investigação criminal leve a conclusões equivocadas, valendo lembrar episódio recente, na Dinamarca, em que 32 presos foram libertados em razão de falhas em indícios de geolocalização de celulares. No caso, a própria polícia detectou falhas de omissões de dados em processos de conversão de dados, tornando os registros de ligações e de geolocalizações incompletos, além de sistemas que mostravam os dispositivos conectados a diversas estações radio bases ao mesmo tempo, com erros na faixa de quilômetros[14].

Por fim, vale notar a distinção feita pela jurisprudência alemã entre interceptação de telecomunicação, de um lado, e infiltração online, de outro. O regime jurídico do processamento e armazenamento de dados difere-se assim do regime do processo de telecomunicações. Essa distinção decorre especialmente do julgado do Tribunal Constitucional Alemao de 2008 das investicacoes online (Online-Durchsuchung)[15] e

da consequente alteração do código de processo penal em seu § 100b StPO, em 2017. Assim como em 1983, no famoso julgado do censo, no qual o Tribunal constitucional alemão criou o direito fundamental a autodeterminação informativa, no julgado de 2008 sobre investigações online, o tribunal criou outro direito fundamental nomeado como "Direito fundamental da garantia da confidencialidade e integridade dos sistemas de tecnologia da informação" (*Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme*) [16]. Enquanto o primeiro toca o acúmulo de dados pela administração estatal, o segundo toca o acúmulo de dados pelo estado para investigação penal. Pela potencialidade lesiva maior de investigações baseadas em dados, há, no contexto alemão, uma necessidade maior de justificação de medidas (e reserva legal qualificada) em detrimento do processo dentro do regime jurídico das telecomunicações (p.e. interceptação telefônica), pois a primeira abre um leque maior de possibilidade ao se criar perfis completos de indivíduos[17].

No caso do ordenamento jurídico brasileiro, a privacidade tem sede constitucional *na inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas* (art. 5º, X, CF) e *do 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. 5º, XII, CF).

Dentro desse arquétipo constitucional, sua regulamentação é dada hoje – ainda considerando um cenário pré-LGPD[18] —pelo Marco Civil da Internet (Lei nº 12.965/2014) e seu Decreto Regulamentador (Decreto nº 8.771/2016), de forma parcial, cujo texto legal do Marco Civil estabelece para provedores de aplicações, como o Google, a obrigação da guarda de registros de acesso às suas aplicações pelo prazo de seis meses, prorrogável, cautelarmente, a requisição do Ministério Público, autoridades policiais ou administrativas (art. 15).

Contudo, o Marco Civil da Internet não esclarece sobre a amplitude da utilização dos registros de acesso às aplicações em investigações criminais. A Lei nº 9296/1996, que trata das interceptações de fluxo telefônico, telemático e informático autoriza quebras de sigilo, por ordem judicial, em tempo real por parte das autoridades de investigação, desde que atendidos requisitos materiais (art. 4º), porém há controvérsias quanto à extensão constitucional a conteúdo de comunicações armazenadas em um servidor[19], sobretudo se estiver em país no exterior[20].

Próxima de entrar em vigor, a Lei Geral de Proteção de Dados ressalta a importância do respeito à proteção dos dados pessoais, muito embora excepcione em seu art. 4º, III, "d", as *atividades de investigação e repressão de investigações penais,* que aguardam disciplina própria[21].

Portanto, há um campo de indefinição normativa que o STJ deve suprir pela interpretação. O julgamento recente no qual o STF reconheceu o direito fundamental à *autodeterminação informativa* certamente será um vetor orientador dessa análise.[22] E o resultado do julgamento pelo STJ, por sua vez, poderá orientar as reflexões legislativas sobre a necessária regulamentação da proteção de dados pessoais em investigações criminais.

---

[1] *Michael Mahoney*, The histories of computing(s): in: Interdisciplinary Science Reviews, 30 (2005), S. 119–135;

[2] PIMENTA, Victor Martins; PIMENTA, Izabella Lacerda; DONEDA, Danilo. Onde Eles estavam na hora do crime? Ilegalidade no tratamento de dados pessoais na monitoração eletrônica. IN Revista Brasileira de Segurança Pública, vol. 13. N. 1, Mar.2019.

[3] Vide BRUNTY, Joshua; HELENEK, Katherine. *Social Media Investigation for Law Enforcement*. Londres/ Nova York: Routledge, 2013, p.57.

[4] "Para Beccaria, a utilidade é algo material e concreto, pleno de conteúdo axiológico. Nesta acepção, útil é unicamente aquilo que está a serviço dos direitos da maioria e visa garantir a máxima felicidade ao maior número, o que confere ao conceito uma dimensão adequada às perspectivas jurídicas liberais-burguesas da época" (FREITAS, Ricardo de Brito A. P. Razão e sensibilidade: fundamentos do direito penal moderno. São Paulo: Juarez de Oliveira, 2001, p. 76).

[5] Vide notícias do Superior Tribunal de Justiça publicada em 10 de junho de 2020. Disponível em: http://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/Terceira-Secao-vai-decidir-sobre-fornecimento-de-dados-pelo-Google-na-investigacao-do-caso-Marielle.aspx

[6] The New York Times. *Tracking phones, Google is a dragnet for the police*. 13/04/2019. Disponível em https://www.nytimes.com/interactive/2019/04/13/us/google-location-tracking-police.html

[7] Forbes. *Google hands Feds 1,500 phone locations in unprecedented 'geofence' search*. 11/12/2019. Disponível em https://www.forbes.com/sites/thomasbrewster/2019/12/11/google-gives-feds-1500-leads-to-arsonist-smartphones-in-unprecedented-geofence-search/#6e915d4127dc

[8] Facebook sued by Australian information watchdog over Cambridge Analytica-linked data breach. Disponível em https://www.theguardian.com/news/series/cambridge-analytica-files.

[9] Ver https://oag.ca.gov/privacy/ccpa.

[10] Ver https://energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/documents/Google.2019.4.23.%20Letter%20to%20Goog

[11] WASSOM, Briam. *Augmented reality law, privacy, and ethics: law, society and emerging AR technologies.* Waltham: Elsevier, 2015, p.67.

[12] A exemplo, ver https://www.zeit.de/datenschutz/malte-spitz-data-retention

[13] Ver DUARTE, Fábio; FIRMINO, Rodrigo. Espaço, visibilidade e tecnologias: (Re)caracterizando a experiência urbana IN Vigilância e Visibillidade: espaço, tecnologia e identificação, Fernanda Bruno, Marta Kanashiro, Rodrigo Firmino (org.), São Paulo: Ciber Cultura, 2010.

[14] The Guardian. *Denmark frees 32 inmates over flawed geolocation revelations*. 12/09/2019. Disponível em https://www.theguardian.com/world/2019/sep/12/denmark-frees-32-inmates-over-flawed-geolocation-revelations

[15] BVerfGE 120, 274 – 350. A proteção reconhecida pela Corte Constitucional alemã em 2008 incide em casos que compreendem sistemas informacionais que contenham dados pessoais de determinado indivíduo, de modo a criar um perfil em violação à sua pessoa. Por essa decisão são reconhecidos novos riscos à personalidade do indivíduo, extinguindo a linha divisória que separava o corpo físico do 'corpo eletrônico'. Não há mais objetos distintos de proteção, mas um único: a pessoa em suas várias configurações, gradualmente determinada por sua relação com as tecnologias.

[16] Sobre esse novo direito fundamental ver, Hoffmann-Riem, Proteção aos Direitos Fundamentais da Personalidade no Âmbito da Comunicação Digital, em: Ricardo Campos, Georges Abboud, Nelson Nery (Orgs.) Protecao de dados e regulacao,Revista dos tribunais, Sao Paulo 2020 (no prelo).

[17] Não fosse esse alargamento, seria possível que uma autoridade que tivesse acesso a determinado sistema pudesse ter conhecimento de um extenso conjunto de dados, sem estar submetido a limites acerca do seu tratamento. Sobre o assunto veja Gabriele Britz, Freie Entfaltung durch Selbstdarstellung. Mohr Siebeck, Tübingen 2007, p. 51 ss. E ainda, veja Fabiano Menke, A proteção de dados e o novo direito fundamental à garantia da confidencialidade e da integridade dos sistemas técnico-informacionais no direito alemão. In: (Coords.) Gilmar Ferreira Mendes; Ingo Wolfgang Sarlet; Alexandre Zavaglia P. Coelho. Direito, inovação e tecnologia. v.1. São Paulo: Saraiva, 2015, p.205.

[18] Sobre a diferença do tratamento de sigilo de dados pré e pós LGPD vide ABREU, Jacqueline de Souza. Tratamento de dados pessoais para segurança pública: contornos de um regime jurídico

[19] Outras Leis também compõe o palco de debate dessa temática tais como a Lei 13.344/2016 que alterou o Código de Processo Penal para incluir o artigo 13-B: "Se necessário à prevenção e à repressão dos crimes relacionados ao tráfico de pessoas, o membro do Ministério Público ou o delegado de polícia poderão requisitar, mediante autorização judicial, às empresas prestadoras de serviço de telecomunicações e/ou telemática que disponibilizem imediatamente os meios técnicos adequados – como sinais, informações e outros – que permitam a localização da vítima ou dos suspeitos do delito em curso", e ainda a Lei nº 12.850/13 (art. 17).

[20] Tratado na Ação Direta de Constitucionalidade (ADC) 51 em trâmite no STF.

[21] Atualmente, discute-se a elaboração de texto de anteprojeto de lei para a confecção de legislação específica para o tratamento de dados pessoais no âmbito de segurança pública, investigações penais e repressão de infrações penais. Para tanto, pelo Ato do Presidente da Câmara dos Deputados, de 26 de novembro de 2019, foi instituída comissão de juristas destinada a elaborar citado anteprojeto de lei.

[22] ADI 6387 MC/DF. Sobre o julgamento do caso IBGE veja artigo "A proteção de dados pessoais no STF e o papel do IBGE" de autoria de Juliano Maranhão, Ricardo Campos e Juliano Abrusio, publicado pelo Conjur em 29.05.2020. Disponível em: < https://www.conjur.com.br/2020-mai-29/maranhao-campos-abrusio-protecao-dados-stf-ibge>

Juliana Abrusio é diretora do instituto LGPD, doutora em Direito e professora da Universidade Presbiteriana Mackenzie. Sócia da Opice Blum, Bruno, Abrusio e Vainzof Advogados Associados.

Juliano Maranhão é diretor do instituto LGPD, professor Livre-Docente da Faculdade de Direito da USP, membro do Comitê Diretor da International Association of Artificial Intelligence and Law e pesquisador da Fundação Alexander von Humboldt.

Ricardo Campos é diretor do instituto LGPD (Legal Grounds for Privacy Design) e docente assistente na Goethe Universität Frankfurt am Main (ALE).

Nuria López é pesquisadora do Instituto LGPD. doutora em Teoria e Filosofia do Direito pela PUC-SP, advogada em Direito Digital e Proteção de Dados no Opice Blum, Bruno, Abrusio e Vainzof Advogados Associados.

Revista **Consultor Jurídico**, 7 de julho de 2020, 16h02