A Busca Reversa por Dados pe Localização na Jurisprudência do Superior Tribunal de Justiça: Análise Crítica do Rms 61.302/Rj

Gianluca Martins Smanio
Universidade de São Paulo

RESUMO

O desenvolvimento das tecnologias da informação permitiu à autoridade policial utilizar-se de dados pessoais para investigar indícios de autoria e materialidade delitiva no decorrer do inquérito policial. Contudo, a busca por tais dados, como é o caso da informação quanto a localização, envolve restrição a direitos fundamentais do investigado, como a privacidade e o sigilo da comunicação dos dados, que são tutelados pela Constituição Federal/88 – CF/88. Ainda, a regulamentação no direito brasileiro é esparsa e omissa, em especial no que se refere à busca reversa por dados de localização, que visa obter o Internet *Protocol* de alguém que esteve no local do crime, na hora do crime, obrigando o Superior Tribunal de Justiça a debruçar-se e buscar regulamentar o meio de obtenção de prova de acordo com o que a lei dispõe. Cabe apontar que essa aplicação analógica pode trazer questionamentos, que merecem ser analisados criticamente.

Palavras-Chave: Dado de localização. Meio de obtenção de prova. Investigação digital. Busca reversa. Superior Tribunal de Justiça.

1. Introdução

O desenvolvimento das tecnologias da informação que culminou na criação dos smartphones revolucionou o acesso à internet. Segundo dados da pesquisa "Tecnologias da Informação e Comunicação – TIC Domicílio", realizada pelo Comitê Gestor da Internet no Brasil, em 2018, o celular foi o equipamento preferido pelos brasileiros para acessar a rede mundial de computadores. Segundo o estudo, dos domicílios com acesso à internet, o equipamento estava presente em 99,2% dos domicílios para este fim. A título de comparação, o uso do notebook com o mesmo objetivo vem em seguida, em 48,1% dos domicí-

Recebido em 04 de março de 2021.
Aceito em 26 de abril de 2021.
Brasília, v. 12, n. 5 , p. 49-76,maio/ago. 2021
ISSN 2178-0013
ISSN Eletrônico 2318-6917

lios. O acesso aos celulares modernos e a sua portabilidade permitem que o usuário tenha uma conexão perene e constante com a internet, seja para navegação web, comunicação ou geolocalização.

Importante mencionar que o usuário, ao interagir com a internet, deixa um rastro de informações, pessoais ou não, que permitem identificar a pessoa e o uso do aparelho. Seja por meio dos dados pessoais entregues para cadastro em sites, de maneira consentida, seja a geração de dados de *Internet Protocol – IP*, por exemplo, a cada acesso à internet realizado por aquele celular, esses dados são importantes fontes de informação para quem os detiver, ou para a autoridade pública que os requisitar.

Um desses dados é o dado de localização, que, com a possibilidade de conexão com a internet caber no bolso, ganha uma nova relevância, em especial para a investigação policial. Dependendo da técnica utilizada, permite à autoridade policial apontar o local que determinada pessoa estava em horário delimitado, através da triangulação do sinal de acordo com a interação do celular com a Estação Rádio Base – ERBs, ou através de históricos de uso de aplicativos de geolocalização, como o *Waze* ou o *Uber*. Em outros casos, permite o acompanhamento da geolocalização em tempo real do indivíduo, permitido por aplicativos como *Google Maps*, por exemplo. Ainda, há casos, como o que será abordado no presente artigo, denominado busca por dados de localização reversa, que visa descobrir, naquele determinado espaço e horário, quais pessoas estavam presentes com seus celulares, a fim de inserir o suspeito no local do crime, na hora do crime. Como se depreende desses exemplos, são formas diferentes de restrição à privacidade da pessoa investigada, que merecem o devido tratamento legal específico.

No entanto, na legislação brasileira, o tratamento dado a esse meio de obtenção de prova não está consolidado, o que forçou a jurisprudência, em especial à do Superior Tribunal de Justiça – STJ, a analisar os casos em que a busca reversa de dados de localização foi solicitada e/ou utilizada pela autoridade policial no contexto do inquérito policial, e ponderar a eficiência probatória que o método permite, com a limitação ao direito fundamental à privacidade do investigado.

Destarte, o objetivo do presente trabalho é apresentar a proble-

mática da busca reversa por dados de localização no direito brasileiro. Primeiramente, será abordado o direito à privacidade, e delimitar as hipóteses de limitá-la em inquéritos policiais, por meio de métodos ocultos de investigação. Na segunda parte, será conceituado o dado de localização e o tratamento jurídico que recebe da doutrina e da legislação brasileira. Por fim, a jurisprudência do STJ será analisada criticamente, a fim de se observar como o Judiciário está lidando com essa nova técnica investigativa, permitida pelo desenvolvimento da tecnologia da informação.

2. Tutela Constitucional da Privacidade de Dados

Os dados têm relação intrínseca com o direito à privacidade previsto na Constituição Federal (1988), em seu artigo 5º, X. O texto constitucional prevê que são invioláveis a intimidade, a vida privada, a honra e a imagem do indivíduo, garantindo indenização nos casos em que for comprovada a sua violação. Segundo Moraes (2013, p. 54), o direito à privacidade teria como propósito tutelar as relações pessoais e profissionais que o indivíduo gostaria de manter restrita ao conhecimento público. Nesse sentido, teria o direito constitucional de não ser alvo de observação de terceiros, sejam particulares ou o Estado, e manter as suas informações particulares fora do conhecimento público (MORAES, 2013, p. 54). A intimidade, por sua vez, abrangeria situações como relacionamentos familiares próximos e amizades íntimas. Sem a privacidade, não há como o indivíduo desenvolver livremente a sua personalidade (MENDES; BRANCO, 2020, p. 391).

Cabe pontuar que a privacidade, enquanto o direito fundamental que conhecemos hoje, originou-se no longínquo ano de 1890, nos Estados Unidos da América. Em um artigo denominado "*The right to privacy*", ou "o direito à privatividade"[1], Samuel Warren e Louis Brandeis, (1890), definem o direito de ser deixado só, sem que haja interferência de terceiros, enquanto o cerne da privacidade. O motivo do trabalho foi principalmente oferecer uma resposta das camadas

1 Paulo José da Costa Jr. (2011, p. 17), em sua tese de titularidade, aponta que a tradução de privacy deveria ser privatividade para o português, e não privacidade, uma vez que a ideia de privativo na gramática lusitana é mais próxima da ideia transmitida pela ideia de privacy.

mais altas da sociedade à incessante perturbação que os tabloides norte-americanos realizavam na época. Essa forma elitista, individualista e majoritariamente patrimonialista de entender a privacidade norteou a interpretação jurídica do direito fundamental até meados dos anos 1960. Conforme o Estado de Bem-Estar Social foi estabelecido na sociedade mundial pós Segunda Guerra Mundial, a essência da relação entre o cidadão e o Estado modificou-se, sendo possível observar uma expansão do conceito de privacidade, de índole mais coletiva, reconhecendo que grupos sociais mais vulneráveis também poderiam ter a sua privacidade violada. Ante a exigência social por mais direitos sociais e políticos, o Estado foi obrigado a fornecer serviços públicos e, a fim de promover programas sociais, manteve um cadastro social que, aliado a um desenvolvimento tecnológico ainda incipiente, permitia a transmissão e armazenamento de informações em volumes cada vez maiores. Dessa forma, a ideia individualista de privacidade começou a expandir-se para além das camadas mais ricas, abrangendo a sociedade por inteiro, e as informações começaram a ganhar um papel mais central (DONEDA, 2019, p. 33).

Ressalta-se o desenvolvimento das tecnologias da informação, interferindo diretamente nos fluxos de informação e na análise qualitativa e quantitativa das informações coletadas (DONEDA, 2019, p. 35). Em especial com o desenvolvimento da internet a partir do final dos anos 1980 como nova forma de comunicação global, superando as fronteiras geográficas e temporais, o direito à privacidade sofreu modificações em suas relações e interesses, saindo do axioma patrimonialista pessoa-informação-segredo que regia o princípio desde o *right to be left alone*, ingressando no paradigma de pessoa-informação-circulação-controle. Hoje em dia, faz mais sentido definir a privacidade não mais como um direito de estar só, mas sim, dentro do contexto da Sociedade da Informação, reconhecê-la, nas palavras de Stefano Rodotà (2009, p. 15), enquanto "o direito de manter o controle sobre suas próprias informações e de determinar a maneira de construir sua própria esfera individual".

Surge então um dos direitos mais relevantes na discussão de tutela dos dados: a autodeterminação informativa. Teve sua origem no julgado da Corte Constitucional Alemã de 1983 (BVerfGE 65, 1). Nele, a autodeterminação informativa foi construída enquanto parte do direito geral de personalidade, e teria como principais frentes a tu-

tela individual (i) da decisão quanto a divulgação e uso dos dados pessoais, (ii) da decisão dos limites de divulgação sobre sua vida pessoal, e (iii) do conhecimento sobre suas informações (MENKE, 2015)[2]. Essa decisão colocou em destaque que a tutela dos direitos fundamentais deve acompanhar o desenvolvimento tecnológico e potenciais restrições que a técnica permite. Nesse contexto, a partir do enfoque ao tratamento de dados, mais do que para a sua natureza, há clareza no sentido de que não se pode falar em dados insignificantes.

Na transposição para o direito brasileiro a doutrina já apontava que a proteção de dados é um direito fundamental originário da análise conjunta dos princípios constitucionais da dignidade da pessoa humana, da inviolabilidade da intimidade e da vida privada, e da importância da previsão a nível constitucional do *habeas data* (SCHERTEL MENDES, 2018, p. 188). Sendo assim, o Supremo Tribunal Federal, ao referendar a medida cautelar nas Ações Diretas de Inconstitucionalidade n.º 6387, 6388, 6389, 6393, 6390, em 07 de maio de 2020, suspendeu a Medida Provisória n.º 954/2020, que obrigava as operadoras de telefonia a enviar ao Instituto Brasileiro de Geografia e Estatística –IBGE dados armazenados por ela dos seus usuários de telefonia móvel, além do número de celular e do endereço, a fim de auxiliar na produção de estatística oficial, ao reconhecer expressamente o direito à proteção de dados pessoais como garantia constitucional. Em atenção a essa discussão doutrinária e jurisprudencial, há uma Proposta de Emenda Constitucional – PEC n.º 17/2019, que visa incluir no artigo 5º, XII, parte final, a previsão expressa de tutela constitucional da proteção de dados.

Depreende-se do direito à autodeterminação informativa uma esfera subjetiva e outra objetiva. Sobre a dimensão subjetiva, deve-se considerar a autodeterminação informativa como regra, devendo ser afastada de maneira excepcional, apenas quando houver justificativa para tanto. Assim, subdivide-se em subprincípios, que visam tutelar os dados pessoais em todas as suas frentes, sendo eles, segundo Doneda (2019, p. 181-182) (i) o princípio da transparência, exigindo publicidade dos bancos de dados; (ii) princípio da exatidão, exigindo

2 Tal decisão não foi isenta de críticas. Segundo Danilo Doneda (2019, p. 170), a doutrina na época questionou a interpretação a ser dada ao termo "autodeterminação", por tratar-se de uma expressão multifacetada, ainda com uma forte tradição patrimonialista, remetendo ao direito de propriedade.

que todos os dados armazenados devem corresponder à realidade, incluindo a previsão de atualizações necessárias; (iii) princípio da vinculação à finalidade, no qual qualquer utilização de dados pessoais deve obedecer à finalidade informada anteriormente à coleta, limitando a transmissão de dados à terceiros, representando marco valorativo claro de identificação do uso abusivo de dados pessoais; (iv) o princípio do livre acesso do titular, a qualquer momento, a bancos de dados que contenham suas informações, permitindo o controle de seu conteúdo, inclusive por meio da correção e inserção de informações; e (v) o princípio da segurança lógica e física, exigindo proteção aos dados coletados contra extravios, modificação, destruição, acesso não autorizado e transmissões indevidas .

Por sua vez, no que se refere à dimensão objetiva, há obrigação do legislador de agir de maneira positiva, criando meios de tutelar a autodeterminação informativa, seja por meio de procedimentos para coleta e tratamento, seja por meio da proteção contra seu uso indevido. Primeiro, deve ser garantido o conhecimento efetivo do titular de dados em relação a coleta e circulação, inclusive por meio da judicialização da demanda; e a outra, por meio da criação de agências reguladoras de fiscalização do cumprimento da normativa de proteção de dados e seus princípios que, no Brasil, se materializou pela criação da Autoridade Nacional de Proteção de Dados, regulamentado pelo Capítulo IX da Lei Geral de Proteção de Dados (BIONI, 2020).

A nível de legislação federal, a autodeterminação informativa já está expressamente prevista no nosso ordenamento jurídico no artigo 2º, II, da Lei 13.709/2018 (Lei Geral de Proteção de Dados – LGPD). No entanto, o próprio texto legislativo é claro ao prever que os dispositivos da Lei Geral de Proteção de Dados não são aplicáveis ao tratamento de dados com fins de investigação ou repressão de infrações penais, no artigo 4º, III, "d". O §1º do mesmo dispositivo exige a criação de regulamentação específica para o tratamento com esta finalidade, sendo respeitados os princípios do devido processo legal, os princípios gerais de proteção e os direitos do titular previstos. Nesse sentido, no dia 05 de novembro de 2020, a comissão de juristas responsável por elaborar o anteprojeto de Lei Geral de Proteção de Dados para tratamento de dados pessoais com finalidade de segurança pública e investigação penal apresentou o texto ao Presidente da Câmara

à época, o Deputado Rodrigo Maia (DEM-RJ). Até o momento de desenvolvimento do presente artigo, não houve novo desdobramento no Legislativo quanto ao anteprojeto. De toda forma, resta clara a necessidade de respeito da proteção dos dados pessoais na fase preliminar e judicial da persecução penal.

3. Delimitação Conceitual do Dado de Localização

Os dados de localização abrangem principalmente a localização conforme a distância da Estação Rádio-Base – ERB, que confere área de cobertura por meio de antena ou outra forma similar, tanto de sinal de celular como de internet móvel, permitindo a localização aproximada do indivíduo investigado ou da vítima quando realiza ligações telefônicas ou transmite comunicações telemáticas (LOPES JÚNIOR, 2019, p. 150). Essa localização pode ser em tempo real, ou demonstrar localidade passada armazenada, podendo ser relevante para encontrar uma vítima em cativeiro, ou inserir o suspeito no local do crime. Importante ressaltar que, com a conexão existente do aparelho celular com a internet móvel, além desse dado obtido via ERB, há aquele dado de localização que está genericamente vinculado a algum aparelho eletrônico, como o *Global Positioning System* – GPS, geradas com a utilização dos aplicativos *Google Maps*, *Waze* e *Uber*, por exemplo, que ficam armazenados no histórico do aplicativo, gerados pela posição global via satélite.

Dessa forma, é preciso inserir na classificação doutrinária e legal essas diferentes formas de dado de localização, a fim de conseguir pontuar especificamente o grau de restrição que a sua obtenção pela autoridade policial acomete os direitos fundamentais da privacidade e do sigilo das comunicações.

3.1 Classificação doutrinária

De acordo com a Convenção de Budapeste sobre o Cibercrime, em seu artigo 1, "b", dado informático[3] é "qualquer representação de

3 Há dissidência quanto ao conceito de dado digital e dado informático na área da Informática, mas

fatos, informações ou conceitos em forma suscetível de processamento em um sistema informático, incluindo um programa capaz de permitir um sistema informático de desenvolver uma função". O dado pode ser considerado uma fonte de prova digital[4], e a fim de ser transportado ao procedimento judicial, deve ser alvo de meio de prova[5] pericial. Uma vez periciado o dado, já como elemento de prova[6], pode ser utilizado pelo Ministério Público – MP para a formação da opinião delitiva, assim como pode ser objeto de análise judicial para a formação do resultado probatório[7].

Podem conter informações pessoais, seja do usuário, do aparelho informático, do conteúdo e/ou do tipo da conversa telemática realizada entre os interlocutores, e é exatamente por isso que possuem valor para a investigação criminal, em especial para formação da opinião delitiva, na justificativa quanto aos indícios de autoria. Não somente, esses mesmos dados podem fazer parte do processo comunicativo ou não, sendo considerados estáticos, fazendo com que incida proteção diferente conforme a sua situação de fato. Se estático, protegido será pelo direito à privacidade do titular e aos direitos de personalidade; se em comunicação, será protegido por força do sigilo às comunicações.

Na tentativa de classificá-los, a doutrina (PINHEIRO, 2020; BIONI, 2020; DONEDA, 2019) buscou organizar os dados pessoais de acordo com o nível de informações referentes ao seu titular que forne-

---

para o limite do presente trabalho, também serão vistos enquanto sinônimos. Por exemplo, Gregório Guardia (2014, p. 122) aponta que o dado digital é uma noção mais técnica de todos aqueles dados que não têm suporte em computador, como é o caso dos dados informáticos, remetendo ao conceito de suporte digital numérico como unidade constitutiva da informação, como são as mensagens transmitidas por Whatsapp e por sistemas de GPS (Global Positioning System).

4 Fonte de prova, segundo Antonio Magalhães Gomes Filho (2005, p. 308), existe anterior e exteriormente ao processo. Consiste nos objetos (fontes reais) ou seres (fontes pessoais) das quais possa se obter elementos de prova para poder verificar um fato. Por exemplo, uma fonte real seria um computador, enquanto a fonte pessoal seria uma testemunha.

5 Os meios de prova referem-se a uma atividade endoprocessual que se desenvolve perante o juiz, com o conhecimento e participação das partes, visando a introdução e a fixação de dados probatórios no processo (GOMES FILHO, 2005, p 309).

6 Elemento probatório, para Gustavo Badaró (2020, p. 432) é o dado bruto extraído da fonte de prova, mas que ainda não foi valorado pelo juiz.

7 Resultado probatório nada mais é do que a conclusão tomada pelo magistrado, após um processo intelectual de análise dos diversos elementos de prova obtidos, de sua pertinência para a causa e da confiabilidade da fonte de prova para a confirmação ou negação da hipótese da causa (BADARÓ, 2020, p. 432)

cem, independentemente de estarem em comunicação ou não. Primeiramente, há os dados sensíveis, em seguida os dados pessoais em sentido estrito e, por fim, dados públicos. Aqui há a diferenciação dos chamados direitos de personalidade e privacidade, dentro do contexto do artigo 5º, X, da Constituição Federal/88. A mesma doutrina (PINHEIRO, 2020) costuma definir dado pessoal enquanto a informação relacionada a pessoa determinada ou determinável8, podendo abranger mais campos do que nome, sobrenome, idade ou endereços, incluindo placas veiculares, perfil de compra, número IP, dados acadêmicos e, inclusive, os dados de localização objeto do presente artigo, desde que relacionados a pessoa natural viva. A definição reduzida também está incluída no artigo 5º, I, da Lei Geral de Proteção de Dados.

De outra forma, os dados também podem ser classificados de acordo com o grau de interferência na intimidade e na privacidade, conforme a natureza do dado analisado (SIDI, 2016). Assim, do menos sensível à intimidade e ao sigilo das comunicações até o mais sensível, temos os dados cadastrais, em seguida os demais dados (excetos os cadastrais), seguido pelos dados de tráfego propriamente ditos e, por fim, o conteúdo humano das comunicações no topo.

Em primeiro lugar, o dado de conteúdo humano é a comunicação em si, materializada pela mensagem de texto, de voz, envio de imagem, vídeo, ou seja, aquilo que o remetente tenha interesse do destinatário ter conhecimento. Pelo seu caráter mais íntimo, e por tratar-se de informação efetivamente comunicada, esses conteúdos estariam protegidos pelo sigilo das comunicações segundo o artigo 5º, XII, da Constituição Federal/88.

Em segundo lugar estão os dados de conexão, denominados dados de tráfego quando vinculados à comunicação humana9. No Brasil, não há um conceito legal do que se entende por metadado, ou dados de tráfego, permitindo um vácuo conceitual que enfraquece a

8 Dado de pessoa determinável, ou identificável, é aquela que, por mais que ainda não tenha sido identificada, o estado atual da técnica permite que se identifique (SOMBRA, 2019, p. 158-159). Logo, um conjunto de dados pessoais de alguém pode permitir, em cadeia, a cada nova informação cruzada, obter outras informações para identificá-la.

9 Luis Sombra (2019, p. 170) conceitua metadados como pegadas digitais relevantes, nos quais dados trazem informações sobre outros dados, e uma vez cruzados com outras informações, tendem a compensar a dificuldade da obtenção do conteúdo.

sua tutela jurídica10. Nesse sentido, somente espécies e exemplos desses dados são nominados e conceituados na legislação nacional. Tendo como exemplo, a Lei n.º 12.850/2013, no artigo 10-A, §1º, I, lista as seguintes espécies de metadados: "informações referentes a hora, data, início, término, duração, endereço de Protocolo de Internet (IP) utilizado e terminal de origem da conexão". No mesmo sentido, o Marco Civil da Internet (Lei n.º 12.965/2014), em seu artigo 5º, IV: "o conjunto de informações referentes à data e hora de início e término de uma conexão à internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados".

Veja-se que as informações sobre o IP dinâmico, duração, data, hora de conexão e desconexão do servidor de e-mail, e conexão e desconexão do servidor de internet são alguns dos dados de tráfego, ou metadados indissociáveis da comunicação, caracterizando a transmissão da comunicação humana. Se caracterizam e indissociáveis são da transmissão de informação entre interlocutores, devem receber a proteção do sigilo das comunicações. Ao mesmo tempo, também existem os dados que são ocasionalmente vinculados à comunicação humana, como é o caso da localização por GPS de um terminal de internet, que só será um dado de tráfego se for obtido em razão da comunicação ou se estiver vinculada a ela. Caso não esteja, trata-se de outro dado, que não estará abarcado pela proteção ao sigilo das comunicações, e sim à privacidade (SIDI, 2019, p. 299).

Por fim, tem-se os dados cadastrais ou afins, que não estão vinculados a nenhuma comunicação. A Lei n.º 12.850/2013 em seu artigo 10-A, §1º, II, conceitua enquanto: "informações referentes a nome e endereço de assinante ou de usuário registrado ou autenticado para a conexão a quem endereço de IP, identificação de usuário ou código de acesso tenha sido atribuído no momento da conexão." No caso em comento, são dados em que o titular, de forma consciente e deliberada, forneceu para algum site ou provedor de aplicativos para criar uma conta e fazer login. Dessa forma, como houve consentimento na entrega desses dados, em tese, não mereceriam proteção do sigilo de

10 A Convenção de Budapeste, em vias de ser ratificada pelo Brasil, por sua vez, define dados de tráfego em seu artigo 1.d, como "quaisquer dados de computador relativos à comunicação por meio de sistema de computador, gerado por sistema computador que seja parte da cadeia de comunicação, indicando a origem, destino, rota, horário, data, tamanho ou duração da comunicação, ou tipo de sistema".

comunicação, recebendo proteção menor no quesito privacidade, mesmo caracterizando dados pessoais (GUARDIA, 2014, p. 135), como nome, telefone, endereço de e-mail, fornecidos pelo titular e coletados pelo site quando se faz a inscrição de acesso ao serviço digital.

Diante disso, percebe-se que os dados, enquanto fonte de prova ou, depois de periciados, enquanto elementos de prova digitais, são importantes para a persecução penal e a sua colheita pode permitir a formação da opinião delitiva do Ministério Público para o oferecimento da denúncia. Como também envolvem direitos e garantias fundamentais do cidadão, a sua colheita deve respeitá-los e seguir os termos da lei, a fim de evitar restrições desproporcionais. No caso específico do presente artigo, os dados de localização podem ser classificados como dados pessoais ocasionalmente vinculados à comunicação e, portanto, estão abarcados pela proteção da privacidade de dados e, em alguns casos, do sigilo das comunicações, caso essa localização esteja vinculada à transmissão de conteúdo comunicativo entre dois interlocutores.

Essa classificação é importante, uma vez que para além da Constituição Federal/88, a jurisprudência, no tocante à tutela de dados, segue entendimento já sedimentado do STF, como no voto proferido pelo Min. Sepúlveda Pertence no Mandado de Segurança n.º 21.729, julgado em 05 de outubro de 1995, e no Recurso Extraordinário n.º 418.416, julgado em 10 de maio de 2006, no sentido de que o dado estático, não comunicado, estaria abarcado pela tutela do artigo 5º, X, da Constituição Federal/88, e não do inciso XII, que tutela o sigilo das comunicações. Nesse sentido, para a autoridade policial obter dados fora do processo comunicativo, bastaria uma autorização judicial prévia para que coletasse os dados no decorrer da investigação, e não lei específica, o que significaria uma proteção mais branda do que aquela despendida para a tutela da transmissão de informações. Contudo, na seara criminal, as decisões judiciais ainda não reconhecem a dimensão coletiva da tutela da privacidade conforme desenvolvida por Rodotà (2008).

3.2 Tratamento legislativo

Destrinchada a classificação do dado de localização, pode-se apontar especificamente qual a legislação infraconstitucional que re-

gulamentará a sua obtenção conforme a sua natureza, seja estática, seja dinâmica. Dessa forma, se vinculada ao conteúdo transmitido entre o remetente e o destinatário, estará abarcada pelo sigilo das comunicações, no artigo 5º, XII, e deve seguir o rito das interceptações de comunicação da Lei n.º 9.296/1996. Se estiver vinculada ao terminal, ou for informação de localização armazenada, o dado obtido estará protegido pela privacidade, insculpida no artigo 5º, X, e será regulamentado por outra previsão legal, aquela do artigo 13-B do Código de Processo Penal.

No entanto, há na doutrina quem defenda (MOURA; BARBOSA, 2020, p. 488 e 497) que dados de localização armazenados, por estarem protegidos genericamente pela privacidade, supostamente uma proteção menor do que a conferida às comunicações em fluxo, poderiam ser alvo de busca e apreensão nos servidores e provedores de aplicação e serviço de internet. No entanto, com a devida vênia, não se pode coadunar com tal entendimento. O dado de localização do indivíduo, como visto, não pode ser reduzido à dicotomia estático/comunicado, sendo também classificado enquanto pessoal, devendo ser protegido inclusive pelos direitos fundamentais da intimidade e privacidade, uma vez que sua análise permite tomar conhecimento, até em tempo real, da localização espacial da pessoa investigada no tempo. Sendo assim, alguns cuidados são de bom tom, em atenção à invasão da privacidade que o tratamento de dados de localização permite.

Com isso claro, pode-se partir para analisar os artigos que regulamentam a obtenção desses dados. Quanto ao dado de localização estático, o artigo 13-B é expresso ao restringir-se aos casos envolvendo tráfico de pessoas. Na doutrina, há quem defenda que tal restrição não deveria ser literal, podendo ser aplicado o meio de obtenção de prova[11] para qualquer crime considerado grave, mediante ordem judicial, uma vez que o interesse investigativo de tais dados avança para além dos interesses específicos de encontrar vítimas (MOURA; BARBOSA, 2020, p. 497). Outros doutrinadores (LOPES JÚNIOR, 2019, p. 150), de forma intermediária, defendem que o rol de crimes previsto no artigo 13-A também é aplicado ao artigo 13-B, em prol da coerên-

11 Para Gomes Filho (2005, p. 308), meio de investigação de prova, ou obtenção de prova, define-se enquanto procedimentos, geralmente, extraprocessuais, conduzidos por outros funcionários, como policiais, que visam conseguir provas materiais. Via de regra, são sigilosos, irrepetíveis e dependem do elemento surpresa para a obtenção de fontes de prova, acarretando, quase sempre, em restrições a direitos fundamentais, carecendo de decisão judicial a fim de fundamentá-la.

cia legislativa, posto que ambos foram inseridos pela mesma lei (Lei n.º 13.344/2016), devendo o dispositivo, então, abranger os delitos de tráfico de pessoas (art. 149-A do Código Penal), redução à condição análoga à escravidão (art. 149 do CP), sequestro e cárcere privado (art. 148 do CP), extorsão com restrição de liberdade da vítima (art. 158, §3º, do CP), extorsão mediante sequestro (art. 159 do CP) e tráfico internacional de crianças (art. 239 da Lei n.º 8.069/1990). Por sua vez, também há doutrinadores (QUITO, 2020, p. 172) defendendo que a interpretação quanto ao crime previsto em lei deve ser feita de forma estrita, em atenção ao fato de o dispositivo legal restringir uma garantia individual.

O artigo 13-B também prevê que o Ministério Público ou a autoridade policial poderão requisitar, submetendo à prévia autorização judicial[12], às empresas prestadoras de serviço de telecomunicação e/ou telemáticas[13] que entreguem os sinais[14], informações, ou outros meios técnicos de imediato, que permitam a localização da vítima ou de suspeito do ilícito em curso. Importante ressaltar o texto do §4º, que prevê que caso não haja manifestação em doze horas por parte do juiz de garantias, o Ministério Público ou delegado podem requisitar tais dados diretamente às plataformas, mediante mera comunicação ao juiz, em caráter excepcional e de urgência. Essa atribuição excepcional de poder às autoridades mencionadas, segundo parte da doutrina (LOPES JÚNIOR, 2019, p. 151), não exclui a possibilidade do juiz posteriormente não decidir em sentido negativo, cassando o ato,

12 Sobre a autorização judicial prévia, importante definir que é a regra, sendo obrigatória na cessão desses dados pela empresa. Isso restou incontroverso em 06 de novembro de 2020, quando o Supremo Tribunal Federal reconheceu, no julgamento da ADI 5.040, por maioria dos votos, a inconstitucionalidade da Lei Estadual do Piauí n.º 6.336/2013, que obrigava as operadoras de telefonia móvel, sem autorização judicial prévia, a entregarem à Polícia os dados de localização de telefones celulares furtados, roubados ou utilizados em atividades criminosas. Segundo os votos dos ministros Dias Toffoli, Luiz Edson Fachin e Luís Roberto Barroso, a lei estadual atenta contra o Código de Processo Penal, em especial no tocante ao artigo em comento, que exige prévia autorização judicial para tanto.

13 Há quem defenda (NUCCI, 2017, p. 109; LIMA, 2017, p. 104) que a requisição direta pela autoridade policial ou ministerial torna a medida absolutamente inconstitucional, uma vez que o juiz deve ser o responsável por enviar o ofício. De maneira contrária (SANTOS; VALE, 2020), existem os defensores de sua constitucionalidade, uma vez que a privacidade não é direito absoluto e não está prevista expressamente na Constituição da República a submissão do direito fundamental à reserva de jurisdição.

14 Sinal, nos termos do §1º deste artigo, é "posicionamento da estação de cobertura, setorização e intensidade de radiofrequência.".

tendo em vista que o juiz é responsável pelo controle de legalidade da medida. Outra parte da doutrina defende a inconstitucionalidade da medida (QUITO, 2020, p. 172), em atenção à restrição de direito fundamental que a medida permite, que sem o controle posterior judicial, configura efetiva prova ilícita[15].

Continua o dispositivo em comento, no §2º, em seu inciso I, que o dado de localização não pode permitir acesso ao conteúdo da comunicação de qualquer natureza e, se o fizer, deve ser respeitada a legislação sobre interceptação das comunicações. Os incisos II e III, por sua vez, expõem que o período de disponibilidade desses dados deverá ser de trinta dias, podendo ser renovado, apenas uma vez, mediante autorização judicial fundamentada, por igual período. Sendo assim, a medida não pode ultrapassar os sessenta dias. Nos casos excepcionais de requisição direta, a prorrogação é inaplicável, uma vez que a própria lei exige reserva de jurisdição. Por fim, o §3º determina que o inquérito policial deverá ser instaurado no período de setenta duas horas, contado do registro da respectiva ocorrência policial. Isso significa que a solicitação de dados pode se dar enquanto primeiro ato investigativo da investigação policial, o que parece temerário.

Ante o exposto, apesar de visar a regulamentação legal da requisição de dados de localização, resta claro que o dispositivo legal possui contradições e lacunas que precisam ser resolvidas. Mesmo com o avanço tecnológico das tecnologias de informação, a lei não faz qualquer diferenciação entre as técnicas de obtenção da localização do indivíduo, que pode ser de diferentes naturezas, armazenada ou em tempo real, com diversos graus de restrição ao direito à privacidade e intimidade, que merecem explicação diante do avanço tecnológico. Uma das formas mais tradicionais é a denominada de Informação da Localização pelo Local da Célula – CSLI, que permite aproximar a posição do dispositivo móvel de acordo com a intensidade do sinal de transmissão entre o aparelho e a ERB. Essa técnica, por ser a mais tradicional e não exigir comunicação em tempo real de dados, parece aquela que o artigo 13-B visou regulamentar. Como apenas permite acesso a

15 Cumpre salientar que o artigo 13-B é alvo da Ação Direta de Inconstitucionalidade n.º 5.642. Segundo a inicial da Associação Nacional das Operadoras Celulares (Acel), a possibilidade de acesso a dados de localização em casos de emergência sem autorização judicial prévia atenta contra o direito à privacidade e à necessidade de reserva de jurisdição.

uma área de cobertura da ERB, não é a maneira mais eficiente de obter o dado geográfico através do celular do investigado. Somente por meio de técnicas como a triangulação[16], que tornam a técnica mais eficiente e utilizável na investigação, que é possível setorizar através do encontro do resultado de força dos sinais de três torres, e localizar com uma certeza razoável o indivíduo.

Por outro lado, outras técnicas mais modernas que são mais eficientes na busca da localização do indivíduo não estão abarcadas e/ou regulamentadas por meio desta lei, apesar da previsão legal "outros meios técnicos"[17]. Saliente-se que, caso a localização, não importa como foi obtida, esteja armazenada em alguma plataforma, pode a autoridade judicial oficiar a empresa que armazena, desde que a decisão seja devidamente motivada, a enviar tais dados para o Juízo.

A primeira delas é a obtenção da geolocalização em tempo real. Funciona através do sistema de GPS, no qual seria possível vigiar em tempo real a localização e o deslocamento de um suspeito, conforme a interação do usuário com o meio digital, seja pelo celular ou pelo sistema nativo do veículo, por exemplo. Por ser obtido mediante posicionamento de satélites e constante comunicação de dados do aparelho, maior precisão e acurácia do que a obtenção da geolocalização por meio das ERBs, exigindo para tanto que o celular esteja com o seu pacote de dados ativado. Por conta dessa necessidade constante de comunicação de dados, em especial no caso de localização em tempo real, essa técnica atenta contra a privacidade, a intimidade e o sigilo das comunicações, e permite à autoridade policial saber exatamente onde a pessoa está naquele momento temporal. Tendo em vista que os celulares modernos possuem, de fábrica, GPS instalado, e muitos aplicativos como *Uber*, *Waze* e *Google Maps*, que estão em constante conexão com a internet, gerando dados de geolocalização em tempo real, o monitoramento em tempo real do investigado é, segundo Geraldo Prado (2020), altamente invasivo. Exatamente por abranger direitos fundamentais sensíveis, inclusive o sigilo da comunicação de dados,

16 Segundo Ana-Maria Roxin (2007, p. 2), a triangulação é uma técnica que permite estimar a direção de chegada do sinal do aparelho móvel pela intersecção da identificação de seu sinal por três ERBs adjacentes.

17 Do ponto de vista contrário, Santos e Vale (2020) defendem que esse dispositivo tem razão de existir exatamente para abranger o avanço tecnológico, que permitiria maior eficiência investigativa para a autoridade policial conforme a acurácia dos dados de localização para encontrar o suspeito.

defende-se que não estaria abarcada pelo dispositivo do artigo 13-B do Código de Processo Penal.

Outra técnica possível se dá pela utilização da triangulação, como nos casos de obtenção da localização pelas ERBs, mas dessa vez da potência entre a conexão do celular com os roteadores de Wi-Fi em ambientes internos de um mesmo local, como um shopping center ou condomínio de casas/apartamentos. Diferentemente do caso das ERB, e se aproximando com a hipótese do GPS, o celular precisa estar com seu pacote de dados e conexão via Wi-Fi ativados, para que possa acessar a internet. Não somente, como está conectado em um roteador, gera um número de IP ao entrar na rede, trazendo outras formas de identificar o usuário, não se restringindo à localização. Assim como no caso do posicionamento global pelo GPS, defende-se que essa modalidade de geolocalização também ultrapassa o escopo do artigo 13-B, uma vez que, por tratar-se de ambientes internos, pode inclusive vir a atingir a inviolabilidade domiciliar para além da autodeterminação informativa, privacidade, intimidade e sigilo das comunicações.

Por fim, o caso objeto do presente artigo, a busca por localização reversa, que merece análise específica. Nessa forma de busca, o juiz requisita ao servidor os IPs de todos os usuários que estavam logados em um local específico, em determinada janela de tempo. Apesar de tratar-se de dado armazenado, a grande questão dessa técnica de obtenção de dados é a quebra do sigilo de dados de terceiros que não tem relação com os fatos investigados, uma vez que os usuários são indefinidos, abrangendo localização e hora. Através do IP, vinculam o dado ao suspeito para inseri-lo no local do crime, na hora da prática do ilícito. Isso seria feito a despeito dos dados de inúmeras pessoas que não teriam relação com a investigação, e que teriam a sua privacidade, em especial sua autodeterminação informativa, violados em prol da eficiência da investigação policial. Por isso, também não está abrangida no espectro do artigo 13-B, do Código de Processo Penal. Em decorrência da sua atipicidade na legislação brasileira, e pela eficiência que traz à persecução penal, foi tema de julgados do Superior Tribunal de Justiça – STJ, que teceu limites e comentários ao meio de obtenção de prova, que merecem ser analisados.

4. O Superior Tribunal de Justiça e a Busca Reversa por Dados de Localização

Diante da ausência de critério legislativo específico, cabe então ao Judiciário, na maioria das vezes, determinar qual a legislação aplicável (ou não) e os requisitos necessários para que seja lícita a utilização de fonte de prova tecnológica pela autoridade policial na fase preliminar da persecução penal.

O Superior Tribunal de Justiça, desde 2017, tem recebido recursos sobre a licitude da utilização, pela autoridade policial, dessa técnica, mesmo sem regulamentação legal. No primeiro caso, o RMS n.º 59.716/RS, de relatoria do ministro Sebastião Reis Júnior, julgado monocraticamente em 19 de dezembro de 2018, a Google impetrou recurso ordinário constitucional em mandado de segurança com pedido liminar para obstar determinação da Sexta Turma do Tribunal de Justiça do Rio Grande do Sul que teria denegado a segurança e mantido a quebra de sigilo telemático de conjunto não identificado de pessoas, unidas pela circunstância de estarem próximas de determinada localização geográfica em um certo lapso temporal, sem individualização ou especificação dos dados, a fim de investigar furto mediante arrombamento de caixa eletrônico. A liminar foi concedida por ferir, em cognição sumária, o artigo 7º, II, do Marco Civil da Internet de pessoas indeterminadas, o que também violaria os artigos 1º, parágrafo único e 2º, I e parágrafo único, da Lei n.º 9,296/1996.

Em outro caso, o TP n.º 292/SP, de relatoria do ministro Antonio Saldanha Palheiro, julgado monocraticamente em 06 de setembro de 2017, a Google impetrou Pedido de Tutela Provisória a fim de atribuir efeito suspensivo ao recurso ordinário em mandado de segurança interposto contra acórdão originário da 4ª Câmara de Direito Criminal do Tribunal de Justiça do Estado de São Paulo. O caso, na origem, era de uma investigação de roubo na qual foi autorizada a quebra de sigilo telemático, para que fosse averiguada a conexão de usuários que se encontravam em determinado local e nas datas delimitadas, determinando ainda que os provedores individualizassem os International *Mobile Equipment Identity* – IMEI dos aparelhos e fornecessem, por conseguinte, dados dos usuários das contas de e-mail, incluindo dados

cadastrais, relações de locais salvos no *Google Maps* e, ainda, histórico de deslocamento nos últimos trinta dias. A tutela provisória foi concedida, sob configuração de perigo de dano e probabilidade do direito.

Por outro lado, no RMS 61.419/SE, de relatoria do ministro Sebastião Reis Júnior, no exercício da presidência do STJ, julgado em 31 de julho de 2019, a Corte Federal se debruçou diante do recurso ordinário constitucional em mandado de segurança impetrado pela *Google* contra acórdão do Tribunal de Justiça do Estado de Sergipe, que manteve a ordem de quebra de sigilo telemático de conjunto não identificado de pessoas que estariam unidas por transitarem em determinada localização geográfica em definido espaço de tempo, especificando, a decisão na origem, requerer os dados de IPs dos usuários da aplicação em determinado local e hora. A liminar, no entanto, não foi concedida. Primeiramente, o ministro especifica que a medida, na verdade, é caso de busca por localização reversa que envolve quebra de sigilo de dados pessoais, sendo parte deles registros de acesso a aplicações de internet, e não se trata de interceptação telemática. O ministro categoriza os dados relativos ao momento de acesso enquanto registro de acesso a aplicações da internet, nos termos do artigo 5º, VIII, do Marco Civil da Internet, e os dados de localização enquanto dados pessoais, nos termos do artigo 14, I, do Regulamento do Marco Civil da Internet. Uma vez que trata-se de requisição de dados pessoais, é possível aduzir da decisão proferida pelo ministro que nos termos do Marco Civil da Internet, segundo o artigo 22, combinado com o artigo 10, §1º, que os dados de conexão em conjunto com dados pessoais podem ser requisitados por autoridade judicial em curso de processo criminal, não exigindo a lei que os potenciais alvos da quebra estejam identificados, bastando que os dados sejam identificáveis.

Para fundamentar esse último ponto de vista, o ministro traz à discussão julgados anteriores, que tinham como objeto a quebra de registros de conexão com ERBs, e autorizam a requisição desses dados pela autoridade, como o *Habeas Corpus* n.º 247.331 do Rio Grande do Sul, julgado pela Sexta Turma, de Relatoria da ministra Maria Thereza de Assis Moura, publicado em 03 de setembro de .2014, o Agravo Regimental no Recurso Especial n.º 1.760.815 do Paraná, julgado pela Sexta Turma, de Relatoria da ministra Laurita Vaz, publicado em 13 de novembro de 2018, para estender o entendimento lá tomado para a

situação do caso, defendendo que o que diferiria as duas situações seria que, naqueles julgados, tratava-se a requisitada de empresa de telefonia, enquanto no caso da *Google,* de provedor de aplicações de internet o que, no seu entender, não são merecedoras de tratamento diverso.

Por fim, negou a liminar por entender que a técnica de investigação não é feita ao arrepio demasiado da privacidade de terceiros, uma vez que os dados de geolocalização não seriam sensíveis, por não captarem o histórico completo dos locais os quais os sujeitos foram. No caso em questão, o juízo de proporcionalidade foi respeitado, uma vez que o espaço foi delimitado a trinta metros, e a janela temporal a 18 minutos, além de o juiz, seguindo o artigo 23 do Marco Civil da Internet, ter tomado providências necessárias para garantir o sigilo das informações recebidas, decretando o segredo de justiça. Por tratar-se de local ermo, com pouca movimentação, o sopesamento entre a gravidade do ilícito (organização criminosa e homicídio) e a privacidade de poucos potenciais terceiros, resultou na autorização do acesso aos dados de localização em determinada hora.

Como se depreende dos julgados acima, o posicionamento do Superior Tribunal de Justiça apresentou-se enquanto indefinido no que se refere à busca reversa por dados de localização, tendendo, mais recentemente, pela sua possibilidade. Contudo, em 2020, parece que a jurisprudência do STJ tende a pacificar-se quanto à quebra de sigilo telemático de dados de geolocalização de usuários em localização geográfica delimitada, em intervalo de tempo determinado.

4.1 O paradigma trazido pelo RMS 61.302/RJ

Com o julgamento do RMS 61302/RJ, de Relatoria do ministro Rogério Schietti Cruz, de 26 de agosto de 2020, que trata da investigação sobre o assassinato da vereadora da cidade do Rio de Janeiro, Marielle Franco, e seu motorista, Anderson Gomes, a 3ª Seção, por maioria dos votos, indeferiu o recurso em mandado de segurança impetrado pelo *Google*, e reconheceu como lícita a decisão proferida pela 4ª Vara Criminal do Rio de Janeiro/RJ, que autorizou a identificação dos IPs que tenham se utilizado do *Google Maps* e *Waze* no período compreendido entre 10 de março de 2018 e 13 de março de 2018, no

endereço localizado à Rua dos Inválidos, 122, bem como dos mesmos dados referentes a quem tenha se utilizado do buscador do Google no período compreendido entre os mesmos dias, para realizar consultas de acordo com as palavras indicadas na decisão.

De início, ressalte-se que o acórdão afastou a aplicação da Lei 9.296/1996, justificando que a identificação de usuários que utilizaram os serviços dos aplicativos em determinada área geográfica não se confunde com o procedimento de interceptação das comunicações, inclusive refutando em seu voto toda a jurisprudência juntada relacionada à interceptação telemática. Segundo a 3ª Seção, os dados de registro delimitados por localização naquele determinado instante temporal são dados estáticos, e por isso, seriam objeto da tutela geral da privacidade, prevista no artigo 5º, X, da Constituição Federal/88.

No caso, requisitou-se o IP armazenado no servidor do aplicativo, que é um dado estático. Nesse sentido, a interpretação do STJ está de acordo com a doutrina e a jurisprudência do Supremo Tribunal Federal – STF, reconhecendo a tutela da privacidade (mais especificamente, da autodeterminação informativa) quando se demonstra necessária a obtenção do IP nesses casos.

Ademais, a Seção, adotando essa visão compartilhada pelo Supremo Tribunal Federal, julgou ser possível afastar a tutela constitucional do sigilo telemático quando presentes circunstâncias relevantes que denotem a existência de interesse público relevante, mediante decisão proferida por magistrado competente, devidamente fundamentada nos termos do artigo 93, IX, da Constituição Federal/88, justificando a necessidade do deferimento da medida para fins da investigação policial.

Ao exigir que a obtenção do IP na busca reversa deve ser previamente submetida à reserva de jurisdição, a fim de restringir o direito fundamental à privacidade do usuário, continua o STJ reiterando o que já está consolidado na jurisprudência e na doutrina quanto à restrição de direitos fundamentais do investigado, não existindo nenhuma inovação jurídica nesse ponto.

A primeira novidade que cumpre analisar é a aplicação do pro-

cedimento inscrito nos artigos 22 e 23 do Marco Civil da Internet, para a busca reversa por dados de localização, que tratam da requisição judicial de registro de conexão ou de acesso a aplicações na internet. O parágrafo único do artigo 22 elenca, enquanto requisitos legais do requerimento, sob pena de inadmissibilidade:

> *I - fundados indícios da ocorrência do ilícito; II - justificativa motivada da utilidade dos registros solicitados para fins de investigação ou instrução probatória; e III - período ao qual se referem os registros.". Segundo o acórdão, não há previsão específica no artigo de individualização quanto às pessoas afetadas na decisão judicial, uma vez que "o objetivo precípuo da previsão legal é possibilitar a identificação do usuário do serviço ou terminal, isto é, possibilitar a descoberta de quem fez uso do serviço ou acessou um determinado terminal, em algum momento e em certa localidade.*

Por sua vez, o artigo 23 estabelece que cabe ao juiz a tomada de providências necessárias para a tutela do sigilo das informações recebidas e da intimidade dos usuários, podendo decretar segredo de justiça.

Segundo o STJ, por tratar-se o IP de um dado estático gerado através da conexão do usuário com a internet, estaria abrangido pelo escopo do artigo 22 acima mencionado. Textualmente, os incisos do artigo não exigem, a título de fundamentação da decisão judicial, a indicação da pessoa alvo da investigação ou a indispensabilidade da medida. Contudo, esse argumento apresenta problemas de compatibilização com a Constituição Federal (1988) e com a Lei Federal. A busca reversa figura como meio de obtenção de prova e, sendo assim, precisa respeitar o princípio da subsidiariedade, por ser medida, por excelência, que restringe direitos fundamentais, seja em maior ou menor grau. Dessa forma, haveria obrigatoriedade de a decisão que autorizou a medida apontar a impossibilidade de se obter essa fonte de prova de outra forma. Assim, para atender ao artigo 93, IX, da Constituição Federal/88, fundamental destrinchar o requisito da subsidiariedade, apontado, no caso concreto, a complexidade de se obter de outras formas a informação de localização do suspeito na hora do crime.

Quanto à delimitação do suspeito a ser alvo desta medida restritiva, a justificativa ofertada pelo STJ de que a medida busca identificar a pessoa que estaria no local do crime e a hora da sua consumação

apresenta a mesma questão. Como a própria medida prevê, o Juízo requisita ao provedor de aplicativos todos os IPs dentro do espaço e tempo delimitados, a fim de, pelos dados de conexão, confirmar quem estaria na localidade durante o momento do crime. Medidas cautelares precisam estar fundamentadas em indícios suficientes de autoria e materialidade delitiva para serem deferidas. Indícios de autoria, como o próprio nome diz, é a existência de elementos suficientes que relacionam determinado suspeito à autoria do crime investigado. Sendo assim, é perfeitamente possível delimitar e identificar o suspeito alvo desta medida, a fim de confirmar se estava ou não no local do crime, uma vez que é requisito legal. A obtenção de milhares de IPs, dados pessoais que identificam a pessoa, permitiria à autoridade policial observar a localização de pessoas que, muitas vezes, possuem nenhuma relação com a investigação ou com os suspeitos investigados. Ao justificar que o dispositivo legal não exige a identificação, uma vez que esse seria o objetivo da medida, o STJ permite à decisão de piso eximir-se de delimitar os indícios de autoria, como toda cautelar, restringindo-se a apontar materialidade delitiva. Assim, outra obrigação da decisão seria descrever e identificar os suspeitos até o momento da investigação.

Mesmo diante dos questionamentos supramencionados, o acórdão julgou ser proporcional o meio de obtenção de prova, não impondo risco desmedido à privacidade e à intimidade do usuário possivelmente atingido pela medida, diante da gravidade e complexidade dos fatos apurados. Inclusive, reputaram que os parâmetros de restrição geográfica e temporal seriam limitadores do alcance da medida.

Em contraponto, o ministro Sebastião Reis, mesmo reconhecendo a possibilidade do pedido judicial das informações geográficas, votou vencido. Reputou o ministro que a determinação judicial visa, precipuamente, a identificação do usuário, mesmo que em primeiro momento não haja essa possibilidade, o que resultaria em invasão à privacidade ao permitir descobrir a localização do usuário, assim como as buscas realizadas na internet neste período. Não somente, considerou a decisão de piso genérica, por não restar devidamente fundamentada a delimitação temporal de quatro dias, assim como estar ausente a justificativa para atingir um número não identificado de pessoas.

Percebe-se que o voto do ministro acolhe melhor as questões

constitucionais e legais apontadas no tocante a autorização da medida. Saliente-se que a busca reversa pela localização de suspeitos é medida restritiva de direitos fundamentais que, mesmo sendo submetida à reserva de jurisdição prévia, deve respeitar os requisitos de cautelaridade e subsidiariedade. Ainda, aponta o ministro questionamento quanto à delimitação temporal, uma vez que não há referências para o que seria considerado razoável. Como a obtenção desses IPs viola a privacidade de quantidade de pessoas que em nada possuem relação com o objeto da investigação, a delimitação temporal deveria ser mais bem fundamentada.

Por consequência, apesar de respeitável e necessária a iniciativa do STJ em visar regulamentar a busca reversa de dados de localização para pessoa, diante da atipicidade legal, o acórdão ainda apresenta pontos a serem melhor debatidos e consolidados em relação à Constituição Federal/88 e à Lei Federal, no que se refere à restrição a direitos fundamentais de meios de obtenção de prova. Destaca-se a dificuldade de produzir uma decisão fundamentada, em respeito à Constituição Federal (1988), diante da inexistência de procedimento legal a nortear uma justificativa condizente com a natureza e especificidades do meio de obtenção de prova.

5. Conclusão

Ante as análises feitas acima, pode-se concluir alguns pontos quanto ao julgado do Superior Tribunal de Justiça e a busca reversa por dados de localização:

1. A privacidade, enquanto direito de estar só, não abrange a complexidade do tema nos tempos atuais. É preciso analisar a privacidade também pelo seu viés coletivo, denominado autodeterminação informativa, que permite ao titular dos direitos também se proteger quanto aos dados e informações que circulam indevidamente na sociedade sobre a sua pessoa.

2. O dado de localização é um dado pessoal, ocasionalmente de comunicação, tutelado pelo artigo 5º, X e XII, da Constituição Federal/88.

3. Apesar de existir no direito nacional dispositivos legais que visam regulamentar a obtenção de dados de localização, a busca reversa por esses dados não está tipificada na legislação processual.

4. O STJ, por maioria, diante da atipicidade do meio de obtenção de prova, julgou ser constitucional e lícito aplicar analogicamente o procedimento de requisição de registro de conexão à busca reversa, previsto no Marco Civil da Internet.

5. No entanto, para que a decisão que autorizou a busca reversa não incorra em nulidade, é preciso estar comprovada a indispensabilidade da medida e a delimitação dos suspeitos alvo da medida, requisitos não presentes no dispositivo do Marco Civil, necessários sob o ponto de vista das garantias individuais do investigado. Por isso, apesar de respeitável e necessária a tentativa do STJ de regulamentar a medida, deve atentar-se, no caso de ausência de tipicidade procedimental na lei, quanto a incoerências de se autorizar medidas restritivas a direitos fundamentais baseada em regramentos analógicos, sem se ater à natureza e às especificidades da medida para o âmbito criminal.

Gianluca Martins Smanio

Mestrando em Processo Penal pela Faculdade de Direito da Universidade de São Paulo Advogado criminalista

The Reverse Search for Location Data in the Jurisprudence of the Superior Court of Justice: Critical Analysis of RMS 61,302 / RJ

ABSTRACT

The development of information technologies has allowed the police authority to use personal data to investigate evidence of criminal authorship and materiality during the police investigation. However, the search for said data, as in the

case of location information, implies restrictions on the fundamental rights of the investigated, such as privacy and confidentiality of data communication, which are protected by the Constitution of the Republic. Even so, regulation in Brazilian law is sparse and silent, especially regarding reverse search of location data, which aims to obtain the Internet Protocol from someone who was at the scene of the crime, at the time. crime, forcing the Superior Court of Justice to know and try to regulate the means of obtaining evidence in accordance with the law. It should be noted that this analog application may raise questions that deserve critical analysis.

Keywords: Location data. Means of gathering evidence. Digital investigation. Reverse search. Superior Court of Justice.

La Búsqueda Inversa de Datos de Ubicación en la Jurisprudencia del Tribunal Superior de Justicia: Análisis Crítico de RMS 61.302 / Rj

RESUMEN

El desarrollo de las tecnologías de la información ha permitido a la autoridad policial utilizar datos personales para investigar pruebas de autoría y materialidad delictiva durante el curso de la investigación policial. Sin embargo, la búsqueda de dichos datos, como en el caso de la información de ubicación, implica restricciones a los derechos fundamentales del investigado, como la privacidad y la confidencialidad de la comunicación de datos, los cuales se encuentran protegidos por la Constitución de la República. Aun así, la regulación en la legislación brasileña es escasa y silenciosa, especialmente en lo que respecta a la búsqueda inversa de datos de ubicación, que tiene como objetivo obtener el Protocolo de Internet de alguien que estaba en la escena del crimen, en el momento del crimen, obligando el Tribunal Superior de Justicia a conocer y procurar regular los medios de obtención de prueba en conformidad con la ley. Cabe señalar que esta aplicación analógica puede plantear interrogantes que merecen un análisis crítico.

Palabras-clave: Dato de ubicación. Medio de investigación de prueba. Investigación digital. Búsqueda inversa; Tribunal Superior de Justicia.

Bibliografia

BADARÓ, Gustavo Henrique. Processo Penal. 8. ed. São Paulo: Revista dos Tribunais, 2020.

BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense, 2020.

COSTA JÚNIOR, Paulo José da. O direito de estar só: tutela penal da intimidade. 4.ed. São Paulo: Revista dos Tribunais, 2013.

DONEDA, Danilo. Da Privacidade à proteção de dados pessoais: fundamentos da Lei Geral de Proteção de Dados. 2. ed. São Paulo, Revista dos Tribunais, 2019.

FERRAZ JUNIOR, Tércio Sampaio. Sigilo de Dados: o Direito à privacidade e os limites à função fiscalizadora do Estado. Revista da Faculdade de Direito da Universidade de São Paulo. São Paulo, v. 88, p. 439-459, jan-dez, 1993.

GOMES FILHO, Antonio Magalhães. Notas sobre a terminologia da prova (reflexos sobre o processo penal brasileiro). In: YARSHELL, Flávio Luiz; MORAES, Maurício Zanoide (Orgs.). Estudos em homenagem à professora Ada Pellegrini Grinover. São Paulo: DPJ Editora, 2005, p. 303-318.

GUARDIA, Gregório Edoardo Raphael Selingardi. Comunicações eletrônicas e dados digitais no processo penal. São Paulo: Max Limonad, 2014.

LIMA, Renato. Brasileiro de. Código de processo penal comentado. Curitiba: Juspodivm, 2017,

LOPES JÚNIOR, Aury. Direito Processual penal. 16.ed. São Paulo: Saraiva, 2019, p. 150.

MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. Curso de Direito Constitucional. 15. ed. São Paulo: Saraiva, 2020, Edição do Kindle.

MENDES, Laura Schertel. Habeas data e autodeterminação informativa: os dois lados da mesma moeda. Direitos Fundamentais & Justiça, Belo Horizonte, ano 12, n. 39, p. 185-216, jul./dez. 2018.

MENDES, Laura Schertel. Privacidade, proteção de dados e defesa

do consumidor: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014. Edição Kindle.

MENKE, Fabiano. A proteção de dados e o novo direito fundamental à garantia da confidencialidade da integridade dos sistemas técnico-informacionais no direito alemão. In MENDES, Gilmar Ferreira; SARLET, Ingo Wolfgang. COELHO, Alexandre Zavaglia P. (coord.). Direito, Inovação e Tecnologia. V. 1. São Paulo: Saraiva, 2015. Edição do Kindle.

MORAES, Alexandre de. Direito Constitucional. 29.ed. São Paulo: Atlas, 2013.

MOURA, Maria Thereza Rocha de Assis; BARBOSA, Daniel Marchionatti. Dados digitais: interceptação, busca e apreensão e requisição. In LUCON, Paulo Henrique dos Santos et. al. (coord.) Direito, Processo e Tecnologia. São Paulo: Revista dos Tribunais, 2020, p. 477-502.

NUCCI, Guilherme de Souza. Código de processo penal comentado. Rio de Janeiro: Forense, 2017.

PINHEIRO, Patricia Peck. Proteção de Dados Pessoais: Comentários à Lei n. 13.709/2018 -LGPD. Editora Saraiva, 2020, Edição do Kindle.

PRADO, Geraldo. Tutela contra a geolocalização contínua. In BRITO CRUZ, Francisco; FRAGOSO, Nathalie (eds.). Direitos Fundamentais e Processo Penal na Era Digital: Doutrina e Prática em Debate. Vol. III. São Paulo. InternetLab, 2020, edição Kindle.

QUITO, Carina. As quebras de sigilo telemático no processo penal e o paradoxo do acesso irrestrito às comunicações armazenadas. In LUCON, Paulo Henrique dos Santos et. al. (coord.) Direito, Processo e Tecnologia. São Paulo: Revista dos Tribunais, 2020, p. 161-185.

RODOTÀ, Stefano. A vida na sociedade da vigilância: a privacidade hoje. Rio de Janeiro: Renovar, 2008.

ROXIN, A. et. al. Survey of Wireless Geolocation Techniques. 2007, Washington: IEEE Globecom Workshops, 2007, p. 1-9, doi: 10.1109/GLOCOMW.2007.4437809.

SANTOS, Cleopas Isaias; VALE, Samyr Béliche. Investigação em tempo real: a Lei n.º 13.344/2016 e as novas técnicas de geolocalizaçào de vítimas e suspeitos de crimes por tráfico de pessoas. In BRITO CRUZ, Francisco; FRAGOSO, Nathalie (eds.). Direitos Fundamentais e Processo Penal na Era Digital: Doutrina e Prática em Debate. Vol. III. São Paulo. InternetLab, 2020, edição Kindle.

SIDI, Ricardo. A Interceptação das comunicações telemáticas no processo penal. Belo Horizonte: Editora D'Plácido, 2016, p. 295

SOMBRA, Thiago Luís Santos. Fundamentos da Regulação da Privacidade e Proteção de Dados Pessoais: Pluralismo jurídico e transparência em perspectiva. São Paulo: Revista dos Tribunais, 2019.

WARREN, Samuel; BRANDEIS, Louis. The right to privacy. Harvard Law Review, v.4, n. 193, 1890.