A QUEBRA DE SIGILO DE DADOS BASEADA EM COORDENADAS GEOGRÁFICAS E O PRINCÍPIO DA PROPORCIONALIDADE

Tiago Dias Maia[1]
Galtiênio da Cruz Paulino[2]

Sumário: 1 Introdução. 2 Visão holística dos direitos fundamentais. 3 Colisão de direitos fundamentais e interpretação. 4 Compatibilidade com as normas internacionais de proteção aos direitos humanos. 5 Compatibilidade constitucional e infraconstitucional. 6 Demonstração prévia de indícios de autoria dos alvos. 7 Princípio da presunção de inocência e inversão do ônus da prova. 8 Utilidade da medida para a investigação criminal e *fishing expedition*. 9 Conclusão.

1 · INTRODUÇÃO

Com o avanço tecnológico, muito se tem debatido sobre a proporcionalidade de medidas de investigação inovadoras em que se utilizam dados pessoais armazenados por provedores de serviços de internet com a finalidade de elucidar crimes.

Provedores de serviço de internet coletam dados o tempo todo dos usuários de seus serviços, inclusive dados de localização. Isso é possível porque os modernos aparelhos utilizados por boa parte das pessoas, como *smartphones*, relógios inteligentes (*smartwatches*) e *tablets,* são capazes de fornecer sua precisa localização através de tecnologias como GPS, redes *wi-fi* e redes de dados móveis.

O Google, atualmente, é o principal usuário deste tipo de ferramenta. A empresa usa informações de localização coletadas de seus usuários com diversas finalidades, como fornecer aos seus usuários recomendações personalizadas baseadas em lugares já visitados, anúncios direcionados, informações sobre o trânsito ou, até mesmo, informar em quais horários um restaurante está mais cheio.

Recentemente, a ferramenta tecnológica chamada em inglês de *geofencing* está sendo utilizada cada vez mais e de maneira mais difundida. *Geofence* pode ser conceituada como um perímetro virtualmente definido ao redor de um certo ponto no

1 Promotor de Justiça (MPDFT). Membro-Auxiliar do Procurador-Geral da República na Assessoria Criminal do Superior Tribunal de Justiça. Ex-Defensor Público. Pós-graduado em Direito Constitucional e em Direito Penal e Processual Penal pela Faculdade de Direito Professor Damásio de Jesus.

2 Procurador da República. Ex-Membro Auxiliar do Procurador-Geral da República na Secretaria da Função Penal Originária no Supremo Tribunal Federal (2018/2019). Membro Auxiliar do Procurador-Geral da República na Assessoria Criminal no Superior Tribunal de Justiça. Doutorando em Direito pela Universidade do Porto (Portugal). Mestre em Direito pela Universidade Católica de Brasília. Pós-graduado em Direito Público pela Escola Superior do Ministério Público da União. Pós-graduado em Ciências Criminais pela UNIDERP. Bacharel em Direito pela Universidade Federal da Paraíba.

globo terrestre, uma espécie de "cerca virtual". É graças a esse tipo de ferramenta que o usuário de um dispositivo móvel equipado com sinal de GPS, ao passar próximo a uma lanchonete, pode receber uma notificação em seu aparelho com algum *voucher* para ser usufruído naquele estabelecimento que contratou este tipo de serviço de empresas de tecnologia.

A tecnologia, que ganhou importância em termos comerciais, mostra-se valorosa em situações nas quais a investigação de crimes graves não avança por falta de elementos que indiquem algum suspeito. Crimes graves como homicídio e estupro, por vezes, são cometidos sem que se possa encontrar elementos de prova que levem a algum suspeito, como testemunhas, filmagens, resquícios de DNA ou impressões digitais, por exemplo; sendo necessária, portanto, a adoção de técnicas especiais de investigação.

Nesses contextos, considerando que atualmente existem dois dispositivos digitais por habitante no Brasil, sendo 234 milhões só de *smartphones*,[3] as autoridades começaram a solicitar de empresas como o Google informações de todos os usuários de seus serviços que estiveram no perímetro que circunda pontos relevantes para a investigação, como o local em que tenha sido encontrado o corpo de uma vítima de homicídio ou o local onde tenham sido achados pertences de uma vítima de roubo.

Em um mandado de quebra de sigilo de dados telemáticos de geolocalização, conhecido nos Estados Unidos como *geofence warrant*, questiona-se ao Google se consta de sua base de dados o registro de algum usuário naqueles locais específicos em uma determinada janela de tempo, geralmente o momento do crime, o que pode levar a uma pista sobre o autor do delito e abrir alguma linha de investigação.

A principal polêmica em relação a este tipo de meio de investigação decorre de serem requisitadas informações de todos os usuários que estiveram no local usando um dispositivo móvel associado a serviços do Google, independentemente de qualquer outra vinculação com o fato criminoso.

Nesse caso, o Estado obteria informações atinentes à privacidade dos indivíduos, que muito provavelmente não cederam seus dados ao Google com a finalidade de serem vigiados, muito menos para produzir elementos em seu desfavor em um processo criminal.

Argumenta-se, ainda, que pessoas poderiam ser acusadas em um crime simplesmente por ter passado pelo lugar errado, na hora errada. Muitos teriam que contratar advogados para explicar às autoridades que, embora estivessem próximos ao local do crime investigado, nada têm a ver com o fato, gerando uma espécie de inversão do ônus da prova.

Além disso, o crime pode ter ocorrido em uma região populosa, de modo que a quebra de sigilo pode atingir dezenas ou até centenas de pessoas que, a princípio, nada fizeram de errado que justificasse a violação de sua privacidade.

Também causa preocupação a possibilidade de utilização desvirtuada da medida por Estados totalitários com intenção de vigiar e controlar sua população e, especialmente, perseguir opositores políticos.

---

3 De acordo com pesquisa realizada por Fernando de Souza Meirelles, "são 424 milhões de dispositivos digitais em uso no Brasil em junho de 2020, sendo 190 milhões de computadores e 234 milhões de *smartphones*. A densidade (*per capita*) de dispositivos digitais era de 50% em 2010, e atinge 200% em 2020, ou melhor, dois dispositivos digitais por habitante" (MEIRELLES, 2020, p. 64).

Há, portanto, evidente colisão entre o direito fundamental da coletividade à segurança pública e o direito fundamental dos indivíduos de não terem violado seu direito à privacidade, mormente sem que haja qualquer indício de autoria contra si.

A colisão de direitos fundamentais demanda uma análise cuidadosa não só dos problemas atuais de relativização mas daqueles que também podem surgir com o uso indiscriminado de medidas invasivas de investigação.

Faz-se necessário, portanto, analisar de forma holística os direitos fundamentais envolvidos, bem como a compatibilidade entre a medida e o ordenamento jurídico brasileiro, para então concluir se a quebra de sigilo de dados telemáticos de localização sem indícios de autoria criminal é medida investigativa legítima.

2 · VISÃO HOLÍSTICA DOS DIREITOS FUNDAMENTAIS

A Constituição Federal forma um sistema aberto, composto por princípios e regras, os quais devem ser compreendidos holisticamente e em perfeita harmonia. Os preceitos fundamentais, dotados de maior valoração axiológica, possuem maior relevância constitucional e servem de paradigma interpretativo aos demais preceitos, devendo, por conseguinte, incidir de maneira plena, sempre compatibilizando possíveis antinomias. Esses princípios estão presentes na Constituição de 1988 na parte denominada "Dos Princípios Fundamentais", os quais, repita-se, devem sempre ser analisados em conjunto e em harmonia com o princípio da unidade constitucional.

Nos Estados democráticos, os direitos fundamentais devem se fazer presentes no topo da hierarquia normativa, ou seja, na Constituição. Eles vinculam todos os poderes, regulam as situações (conteúdo) mais relevantes na sociedade e se encontram na "medida máxima de necessidade de interpretação" (ALEXY, 2015, p. 48).

Para um direito ser considerado fundamental, deve englobar interesses que necessitam ser protegidos e promovidos pelo Direito. Além disso, é necessário que "o interesse ou carência seja tão fundamental que a necessidade de seu respeito, sua proteção ou seu fomento deixe fundamentar-se pelo Direito" (ALEXY, 2015, p. 50).

A fundamentalidade de um direito está presente, portanto, quando ele se apresenta como prioridade no sistema jurídico e, ocorrendo violação ou não, seja promovido, sob pena de se atingir o núcleo existencial do próprio sistema.

Ocorre que a interpretação dos preceitos fundamentais, necessária para uma verdadeira supremacia da Constituição, depende da efetividade desse diploma normativo, advinda da sua eficácia social, voltada para o resguardo dos anseios individuais e coletivos de uma sociedade, mediante uma relação de equilíbrio entre os direitos e garantias fundamentais de ambos, indivíduo e sociedade.

Nesse cenário, o direito, para ser considerado fundamental, deve receber uma especial proteção formal e material. Do ponto de vista formal, o direito fundamental possui sede constitucional, que resulta em barreiras procedimentais mais rígidas para supressão e alteração, em alguns casos absolutas (como as cláusulas pétreas), além de possuírem aplicabilidade imediata. Em termos materiais, tais direitos fazem parte da denominada Constituição Material e estão na base de formação do Estado. Podem ser encontrados em outros diplomas normativos, fora, portanto, da literalidade da Constituição, ou podem mesmo não ser expressos.

Outrossim, os direitos fundamentais variam de acordo com o contexto constitucional. Porém, alguns deles são considerados universalmente fundamentais, como a vida, a liberdade, a dignidade da pessoa humana. O conteúdo desses direitos varia conforme a realidade social em que se encontram, a qual condicionará seu conteúdo.

Esses direitos possuem dupla face, visto que podem ser considerados como direitos subjetivos individuais ou como elemento objetivo fundamental de uma sociedade (SARLET, 2007, p. 166). Além de servirem como mecanismos dos indivíduos ante o Poder Público, os direitos fundamentais são, também, valores constitucionais de caráter objetivo, com eficácia sobre todo o ordenamento jurídico; servem como norte para o atuar de todos os poderes constituídos.

Todos os direitos fundamentais transpassam a esfera do indivíduo. Na perspectiva objetiva, podem-se restringir direitos individuais, ainda que fundamentais, quando o interesse da sociedade prevalecer e desde que respeitado o núcleo essencial. A face objetiva dos direitos fundamentais apresenta-se como um dever imposto ao Estado de concretizá-los e implementá-los. Há a denominada influência objetiva e valorativa dos direitos fundamentais. A dimensão objetiva é autônoma e serve de norte à interpretação e à aplicação do Direito infraconstitucional.

Os direitos fundamentais também se apresentam como dever de proteção do Estado, que deve agir de maneira preventiva na proteção dos particulares diante dele próprio (o Estado) e dos demais particulares. A valorização dos direitos fundamentais na perspectiva objetiva resultou na conscientização da insuficiência de uma concepção dos direitos fundamentais como direitos subjetivos de defesa para a garantia de uma liberdade efetiva para todos, e não apenas daqueles que garantiram sua independência social e o domínio de seu espaço de vida pessoal (SARLET, 2007, p. 177).

Sob o aspecto subjetivo, o indivíduo pode buscar, em juízo, a proteção e observância dos direitos fundamentais, tutelados em face dos Estados e dos demais integrantes da sociedade.

Nesse cenário, o estudo da eficácia dos preceitos fundamentais presentes na Constituição deve focar a diferença entre a eficácia jurídica e a social. Esta última é enquadrada como efetividade da norma (SILVA, 1982, p. 48), ou seja, sua aplicabilidade no plano dos fatos. A "efetividade, em suma, significa a realização do Direito, o desempenho concreto de sua função social" (BARROSO, 2010, p. 221). Apresenta-se como "a materialização, no mundo dos fatos, dos preceitos legais e simboliza a aproximação, tão íntima quanto possível, entre o 'dever-ser' normativo e o 'ser' da realidade social" (BARROSO, 2010, p. 221).

Por sua vez, o estudo da eficácia jurídica dos direitos fundamentais deve ser aferido em consonância com as diversas funções que esses direitos podem assumir. Eles podem ser classificados como direitos de defesa (caso do direito à intimidade) e como direitos a prestações (caso do direito à segurança). Quanto aos primeiros, de caráter subjetivo, não há discussão quanto a sua aplicação (eficácia jurídica) imediata. A discussão sobre a aplicabilidade imediata gira em torno dos direitos fundamentais prestacionais, os quais, em regra, também devem ser entendidos como de aplicabilidade imediata. Essa característica, em verdade, deve ser entendida como inerente a todos os direitos e garantias fundamentais, independentemente da parte na qual eles se localizem no texto constitucional (SARLET, 2007, p. 275). Os direitos

prestacionais são avalizados sob as perspectivas individual e coletiva, que deverão ser consideradas no momento que forem interpretados.

Essa interpretação se adequa à previsão normativa do art. 5, § 1º, da Constituição, contribuindo para evitar o esvaziamento do conteúdo dos direitos fundamentais.

Em razão do referido dispositivo, surge uma presunção, mesmo que relativa, de aplicabilidade imediata das normas de direitos e garantias fundamentais. Essa presunção só pode ser afastada em caráter excepcional e desde que devidamente fundamentada (PAULINO, 2019, p. 35). É obrigação do poder público "extrair das normas que os consagram (os direitos fundamentais) a maior eficácia possível" (SARLET, 2007, p. 235).

Sob essa perspectiva, os direitos fundamentais se apresentam como um conjunto de direitos que norteia e garante a existência dos seres humanos como indivíduos e seres gregários; constituem, portanto, um sistema de proteção a ser respeitado de forma holística. Possíveis antinomias, porém, devem ser solucionadas, necessitando-se de um atuar interpretativo que supera a simples subsunção do fato à norma. Na linguagem do Direito, segundo Alexy, há uma abertura necessária que comporta a "possibilidade de contradições normativas, a falta de normas, sobre as quais a decisão apoiar-se, e a possibilidade de, em casos especiais, também decidir contra o texto de uma norma" (2015, p. 36).

É sob esse enfoque de harmonia dos direitos fundamentais que medidas voltadas ao resguardo da sociedade, como a demonstrada neste artigo, devem ser interpretadas e aplicadas.

3 · COLISÃO DE DIREITOS FUNDAMENTAIS E INTERPRETAÇÃO

Ordinariamente, os direitos fundamentais individuais entram em colisão com os bens coletivos. Esse choque é muito presente no contexto da segurança pública, quando o Estado, objetivando proteger seus cidadãos, ao garantir uma conjuntura de segurança, acaba atingindo o direito à liberdade de algumas pessoas.

Ocorre que os possíveis conflitos entre direitos fundamentais individuais, normalmente do acusado, e direitos fundamentais coletivos, atinentes à sociedade, devem ser solucionados por meio da adoção do entendimento de que nenhum direito fundamental pode ser suprimido por completo em nenhuma hipótese.

Nesse diapasão, surge a necessidade de definir se os direitos fundamentais são regras ou princípios – como mandamentos de otimização, podendo incidir em graus diferentes, a depender dos contextos fático e jurídico. Em sendo princípios, conforme adotado neste artigo, a solução ocorre por meio da ponderação; em sendo regras, são mandamentos definitivos, ou seja, devem ou não ser observadas, resultando: a) na declaração de um dos direitos como válido e o outro como inválido; b) na declaração de um dos direitos como não aplicável; ou c) na fixação de uma exceção em uma das normas.

Como todo princípio é válido, o conflito entre os princípios envolve a "dimensão do peso", ou seja, "aquele que vai resolver o conflito tem de levar em conta a força relativa de cada um" dos princípios (DWORKIN, 2012, p. 43). A controvérsia no julgamento sobre a mensuração exata de um princípio e sobre qual deve prevalecer

em caso de colisão "é parte integrante do conceito de um princípio, de modo que faz sentido perguntar que peso ele tem ou quão importante ele é" (DWORKIN, 2012, p. 43). A solução do conflito ocorre com a fixação da precedência de um princípio, condicionada pelas circunstâncias do caso concreto. Em condições diversas, pode haver resultado diverso (DWORKIN, 2012, p. 43).

De plano, nenhum princípio prevalece sobre outro em tese. A supremacia de um dos princípios em choque, repita-se, depende das circunstâncias/condições do caso concreto, sempre se mensurando os direitos em colisão e buscando-se evitar a completa exclusão de um deles.

Os princípios não possuem obrigações/consequências de cunho definitivo, mas apenas *prima facie*. O âmbito de incidência de seu conteúdo, conforme acima exposto, não se encontra previamente determinado.

Em razão do caráter de preceito constitucional assumido, os direitos fundamentais podem ser restringidos apenas por normas de envergadura constitucional. Essas restrições, segundo Alexy, podem ser realizadas por "normas de hierarquia constitucional ou normas infraconstitucionais, cuja criação é autorizada por normas constitucionais" (2011, p. 286). As restrições infraconstitucionais só são admissíveis quando autorizadas pela própria Constituição. Surgem as denominadas restrições indiretamente constitucionais.

Nesse ponto, aflora a necessidade de um juízo de ponderação por meio do princípio proporcionalidade que, segundo Carlos Pulido (2014), cumpre a função de estruturar o procedimento interpretativo para a determinação do conteúdo dos direitos fundamentais. Tal princípio se faz necessário em razão de os direitos fundamentais serem normativamente indeterminados.

"Nenhuma disposição jusfundamental, por mais específica que pareça, permite que se conheça de plano todas e cada uma das normas que estatui direta ou indiretamente" (PULIDO, 2014). A atuação do princípio da proporcionalidade se dará justamente quando se for concretizar um direito fundamental.

Por sua vez, a ponderação se desenvolve em três etapas sequenciais: a) devem-se comprovar os reflexos do não cumprimento de um dos princípios em conflito, de acordo com o grau de descumprimento; b) deve-se aferir a importância de se cumprir o princípio contrário; c) deve-se comprovar se o cumprimento do princípio contrário justifica que o outro seja prejudicado (ALEXY, 2011, p. 111).

Haverá atuação desproporcional se, diante de princípios em contraposição, não se estabelecer uma relação de balanceamento entre os princípios envolvidos, praticamente suprimindo-se o papel do princípio relegado.

Na aplicação do princípio da proporcionalidade aos direitos fundamentais, deve-se considerar a faceta da proibição da proteção deficiente (PULIDO, 2014). Ao intérprete, caberá aferir se uma atuação estatal, por ação ou omissão, torna vulnerável um direito fundamental. Por meio da proibição de proteção deficiente, permite-se a fixação de um padrão mínimo de proteção aos direitos fundamentais que deve ser observado e promovido pelo Poder Público.

Desse modo, todos os direitos fundamentais devem ser protegidos pelo Poder Público, tanto no momento da elaboração legislativa quanto no da aplicação.

Sempre se deve assegurar o núcleo essencial de todos os direitos fundamentais, que gera um limite às possíveis restrições a que eles podem ser submetidos. Um direito fundamental, em suma, só pode ser restringido se, no momento da restrição, em razão da incidência de outro direito fundamental, for observado seu conteúdo mínimo.

Nessa senda, os sistemas jurídicos de proteção devem se pautar, sempre, pela proteção dos indivíduos e da sociedade, pois os seres humanos são sociáveis por natureza. A concepção que se deve ter de direitos humanos, centrada na dignidade da pessoa humana, só será concebida sob uma perspectiva plena se enfocada sob um contexto social, pois a natureza existencial de todos os direitos passa por uma perspectiva comunitária (DA SILVA, 2015, p. 136).

Desse modo, as interpretações jurídicas de proteção devem se sustentar em uma perspectiva individual e social.

Nesse cenário, ao se aferir o cabimento de uma medida investigativa, voltada à eficácia da persecução penal, deve-se sempre ter em mente que o cabimento da medida deverá aferido por meio de uma interpretação que gere uma relação de equilíbrio entre todos os direitos fundamentais envolvidos, inclusive os que dizem respeito à sociedade e à vítima.

4 · COMPATIBILIDADE COM AS NORMAS INTERNACIONAIS DE PROTEÇÃO AOS DIREITOS HUMANOS

Embora não trate diretamente sobre o tema, a Convenção Americana de Direitos Humanos protege os indivíduos de ingerência arbitrária ou abusiva em sua vida privada, conforme se vê:

> Artigo 11. Proteção da honra e da dignidade
>
> 1. Toda pessoa tem direito ao respeito de sua honra e ao reconhecimento de sua dignidade.
>
> 2. *Ninguém pode ser objeto de ingerências arbitrárias ou abusivas em sua vida privada, na de sua família, em seu domicílio ou em sua correspondência, nem de ofensas ilegais à sua honra ou reputação.*
>
> 3. Toda pessoa tem direito à proteção da lei contra tais ingerências ou tais ofensas. (OEA, 1969, grifo nosso).

O dispositivo é pertinente, considerando que a quebra de sigilo de dados de localização é, sem dúvida, uma ingerência estatal na vida privada da pessoa cujo histórico de localização se revela.

Existe uma preocupação em âmbito internacional sobre o risco de que instrumentos de investigação que se valem de inovações tecnológicas sejam utilizados para espionar e perseguir por parte do Estado, que poderia explorar interpretações equivocadas para dar aparência de legalidade à medida investigativa.

A Corte Interamericana de Direitos Humanos já teve a oportunidade de se debruçar sobre tema parecido (interceptação e monitoramento telefônicos), quando analisou a validade da utilização de inovações tecnológicas na investigação de crimes diante do artigo 11 da Convenção Americana. O seguinte trecho da sentença do caso *Escher e outros* vs. *Brasil* ilustra bem esse ponto:

> 115. A fluidez informativa que existe atualmente coloca o direito à vida privada das pessoas em uma situação de maior risco, devido à maior quantidade de novas ferramentas tecnológicas e à sua utilização cada vez mais frequente. Esse progresso, especialmente quando se trata de interceptações e gravações telefônicas, não significa que as pessoas devam estar em uma situação de vulnerabilidade frente ao Estado ou aos particulares. Portanto, o Estado deve assumir um compromisso com o fim adequar aos tempos atuais as fórmulas tradicionais de proteção do direito à vida privada. (OEA, 2009).

Chamou-se atenção ao papel do Estado de proteger os direitos humanos diante do avanço da tecnologia, obviamente que de maneira conciliatória, isto é, sem colocar empecilhos ao desenvolvimento da ciência.

Neste caso específico, o Brasil foi condenado pela Corte Interamericana por ter violado o direito à vida privada de seus nacionais. Concluiu-se que este tipo de medida deve se basear em uma legislação particularmente precisa, com regras claras e detalhadas, propósito claro, indícios razoáveis de autoria ou de participação, e ser requerida, concedida e fiscalizada por autoridades previstas na legislação de forma fundamentada e com prazo máximo fixado (OEA, 2009).

De fato, há diferenças marcantes entre a medida de quebra de sigilo de dados de geolocalização e a interceptação telefônica, questão debatida no caso *Escher*. Todavia, na falta de debate específico e considerando que ambas as medidas caracterizam sérias interferências na vida privada, é possível valer-se das conclusões obtidas no julgamento como parâmetro para aferir a conformidade da medida em análise com as normas internacionais de proteção aos direitos humanos, pelo menos no que se refere a esse sistema regional.

Neste contexto, ficou claro que, obedecidos certos requisitos que protejam as pessoas de uma ingerência indevida, diligências investigativas que implicam invasão à privacidade são permitidas quando se busca uma relativização do direito individual em prol de interesses legítimos da coletividade, como no caso de investigações criminais.

Há, inclusive, dispositivo expresso neste sentido na Convenção Interamericana, que prevê em seu artigo 32: "Os direitos de cada pessoa são limitados pelos direitos dos demais, pela segurança de todos e pelas justas exigências do bem comum, numa sociedade democrática" (OEA, 1969).

Portanto, a norma internacional, prevendo que certos direitos humanos individuais entrariam em rota de colisão com direitos da coletividade em certas circunstâncias, abriu expressamente a possibilidade de relativização daqueles.

5 · COMPATIBILIDADE CONSTITUCIONAL E INFRACONSTITUCIONAL

Assim como a medida de interceptação telefônica encontra regulamentação constitucional e infraconstitucional, o acesso a dados de localização armazenados por provedores de serviço de internet também encontra regulamentação específica. Os dados pessoais armazenados são protegidos pelo disposto no art. 5º, X, da Constituição Federal, que estabelece como invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas.

Por serem considerados parte da vida privada e da intimidade das pessoas, dados pessoais armazenados por provedores de serviço de internet como o Google devem ser protegidos, cabendo à empresa tomar todas as precauções contra o acesso não permitido a essas informações por terceiros.

Em consonância com o dispositivo constitucional citado, a legislação ordinária cuidou de explicitar essa preocupação, garantindo aos usuários da internet maior segurança na utilização de seus serviços. É o que se pode observar no texto da Lei n. 12.965/2014, conhecida como Marco Civil da Internet:

> Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros. (BRASIL, 2014).

Vê-se, portanto, que o Marco Civil da Internet deixou claro que a guarda de dados pessoais deve atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas. Isso significa que, ao coletar dados pessoais e armazená-los, os provedores tornam-se responsáveis pela guarda daquelas informações e se submetem a todas as consequências desta condição.

O Decreto n. 8.771/2016, que regulamenta o Marco Civil da Internet, traz disposições ainda mais específicas no que tange às obrigações dos provedores de proteção dos dados pessoais por eles coletados, como controle estrito sobre o acesso aos dados e o uso de técnicas que garantam a inviolabilidade dos dados, como encriptação.

Não obstante o cuidado com a manutenção do sigilo, o Marco Civil da Internet prevê expressamente a possibilidade de violação de sigilo desses dados pessoais armazenados, entre outros dados, desde que submetida à reserva de jurisdição (BRASIL, 2014).[4]

O Marco Civil da Internet deixa claro, portanto, que o acesso aos dados pessoais armazenados por um terceiro deve passar pelo crivo do judiciário. O magistrado é quem vai analisar se, naquele caso específico, existe fundamento para que se possa afastar o sigilo dos dados.

Vale lembrar que a permissão legal para autoridades administrativas dada no art. 10, § 3º, da Lei 12.695/2014 é somente a de acesso direto a dados cadastrais, que informem a qualificação pessoal, filiação e endereço.

---

4 Lei n. 12.965/2014: "art. 7º: O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos: [...] II - inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei; III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial; [...]

Art. 10. 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.

§ 1º O provedor responsável pela guarda somente será obrigado a disponibilizar os registros mencionados no *caput*, de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal, mediante ordem judicial, na forma do disposto na Seção IV deste Capítulo, respeitado o disposto no art. 7º" (BRASIL, 2014).

O Decreto n. 8.771/2016 define dado pessoal como "dado relacionado à pessoa natural identificada ou identificável, inclusive números identificativos, dados locacionais ou identificadores eletrônicos, quando estes estiverem relacionados a uma pessoa" (BRASIL, 2016).

Aparentemente, o legislador nacional escolheu separar dados de conexão, em suas diferentes modalidades, de dados pessoais. Assim, um endereço de IP pode não ser considerado dado pessoal, ainda que se trate de informação relacionada à pessoa natural identificável (MELCHIOR, 2014).

De qualquer forma, os dados de localização de pessoas armazenados pelo Google são considerados dados pessoais, seja por se referir a um dado locacional, conforme previsto expressamente no Decreto n. 8.771/2016, seja porque pode revelar informações íntimas daquele usuário.

Além disso, os dados pessoais são de titularidade da pessoa natural a quem dizem respeito. Cabe aos agentes de tratamento apenas o direito sobre a organização de dados pessoais em banco de dados estruturados e sobre a inteligência gerada a partir do tratamento desses dados (CUNTO; GALIMBERTI; LEONARDI, 2019, p. 87).

Sendo assim, fica claro que a legislação infraconstitucional permite o acesso aos dados pessoais de localização armazenados pelo Google, desde que haja prévia autorização judicial, após demonstração do preenchimento dos requisitos a seguir estudados.

6 · DEMONSTRAÇÃO PRÉVIA DE INDÍCIOS DE AUTORIA DOS ALVOS

A principal crítica feita à ordem de quebra de sigilo com base em coordenadas geográficas, ou *geofence warrant,* é a ausência de identificação prévia dos suspeitos cujos dados serão quebrados. Argumenta-se que esse tipo de medida seria uma verdadeira quebra de sigilo exploratória, sem alvos individualizados, não albergada pela ordem jurídica brasileira.

No Brasil, o Google tem manifestado resistência em obedecer às requisições judiciais de dados de localização de seus usuários em investigações criminais e tem ajuizado mandados de segurança contra decisões que o compelem a informar dados à polícia ou ao Ministério Público.

O caso mais célebre é a investigação sobre o homicídio da vereadora Marielle Franco e seu motorista, Anderson Gomes, no Rio de Janeiro. A Justiça do Rio de Janeiro determinou ao Google que fornecesse todas as "*Google accounts*" ou "*Device IDs*" identificadas entre os pontos das coordenadas especificadas, em uma janela de tempo de 15 minutos da data do fato investigado. A partir dos resultados encontrados, o Google deveria encaminhar o histórico de localização (*locations history*) dos dispositivos identificados.

O Google defende que a Constituição e a legislação nacional são incompatíveis com a medida. Sustenta que a Lei n. 9.296/1996 dispõe expressamente em seu art. 2º que o afastamento da privacidade não é admitido sem a demonstração de indícios razoáveis de autoria ou participação.

Todavia, a empresa faz clara confusão com os dispositivos aplicáveis à matéria. Antes de tudo, é preciso esclarecer que a quebra de sigilo de dados com base em

coordenadas geográficas não trata de interceptação de fluxo de dados, mas sim de acesso a dados armazenados.

De forma objetiva, o art. 5º, XII, da Constituição Federal se dirige à comunicação dos dados e não aos dados armazenados em decorrência de uma comunicação anterior. Nesse sentido, o referido dispositivo constitucional é regulamentado pela Lei n. 9.296/1996, que faz referência expressa ao "fluxo de comunicações" (BRASIL, 1996). Portanto, a exigência de demonstração de indícios razoáveis da autoria ou participação do alvo na infração penal apurada é aplicável à técnica de interceptação de comunicações.

De outro lado, na quebra de sigilo com base em coordenadas geográficas não se busca acesso a comunicações em andamento, mas informações coletadas em um certo período de tempo e armazenadas no servidor de um provedor de serviços de internet, isto é, nem mesmo se trata de acesso a dados de comunicação.

A questão foi claramente regulamentada pela Lei n. 12.965/2014. O Marco Civil da Internet, ao regulamentar a possibilidade de acesso aos dados sigilosos mantidos por provedores, define requisitos a serem observados no requerimento e aferidos pela autoridade judicial:

> Art. 22. A parte interessada poderá, com o propósito de formar conjunto probatório em processo judicial cível ou penal, em caráter incidental ou autônomo, requerer ao juiz que ordene ao responsável pela guarda o fornecimento de registros de conexão ou de registros de acesso a aplicações de internet.
>
> Parágrafo único. Sem prejuízo dos demais requisitos legais, o requerimento deverá conter, 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. (BRASIL, 2014)

Verifica-se que não há entre os requisitos a necessidade de apontar indícios de autoria. Isso ocorre porque a principal utilidade dessa medida é revelar a identidade de pessoas que utilizam a internet como meio para a prática de crimes.

A inexigência de demonstração de indícios de autoria tem razão de ser. É que, comumente, os autores de ilícitos cibernéticos não revelam sua real identidade justamente para evitar uma posterior responsabilização. Por esse motivo, a lei prevê a possibilidade de se requisitarem aos provedores de internet dados de conexão, como o IP (*Internet Protocol*), a fim de permitir a identificação dos usuários (JESUS; MILAGRE, 2016).

O principal propósito do *geofence warrant* é justamente encontrar suspeitos em processos nos quais não se tem nenhuma pista sobre a autoria. De fato, seria inviável o cumprimento da medida de interceptação telefônica sem se identificarem os alvos a ser interceptados, razão pela qual, em relação a esse tipo de ferramenta investigativa, é razoável que se exijam indicativos de autoria.

Aliás, o Marco Civil da Internet autoriza o acesso aos dados não só para instrução de processo criminal, mas torna possível que os dados sejam utilizados para instruir processo judicial cível, diferenciando-se mais uma vez da Lei de Interceptações Telefônicas.

No recente julgamento do mandado de segurança interposto pelo Google referente ao caso Marielle, a Terceira Seção do Superior Tribunal de Justiça decidiu pela legitimidade da quebra de sigilo de dados com base em coordenadas geográficas. Entendeu-se que o Marco Civil da Internet não exige a individualização das pessoas atingidas pela quebra. Segundo o relator Rogério Schietti, "tal exigência, por certo, revelar-se-ia verdadeiro contrassenso, na medida em que o objetivo da lei é possibilitar essa identificação" (BRASIL, 2020).

Um dos fundamentos utilizados para permitir a quebra de sigilo foi justamente o fato de os dados serem anonimizados inicialmente. As informações pessoais dos proprietários daqueles dados seriam acessadas posteriormente, com o avanço das investigações e a realização de pedidos específicos.

Para que fique mais claro, é importante conhecer o método utilizado na análise dos dados obtidos por meio desse tipo de quebra. Em linhas gerais, o Google recebe uma requisição de dados sobre uma área próxima ao crime e em uma janela de tempo. Após analisar sua base de dados, o Google identifica os dispositivos encontrados de acordo com os parâmetros definidos no mandado e os envia à autoridade requisitante. Antes desse envio, o Google identifica cada um desses dispositivos com números de identificação anônimos (números ID).

Os investigadores recebem, portanto, apenas dados anônimos e, a partir de então, precisam fazer uma análise de localizações e padrões de movimento, cotejando com outras informações anteriormente colhidas, até que se identifique(m) algum(ns) entre aqueles dispositivos que pareçam relevantes para a investigação.

É possível, ainda, que, entre os dispositivos anonimamente identificados fornecidos inicialmente, os investigadores façam uma filtragem e apontem uma menor quantidade de dispositivos de interesse. Com esses números, solicita-se ao Google a apresentação de dados ainda anônimos, mais abrangentes, podendo abarcar informações de localização fora da área inicialmente delimitada ou até mesmo fora da janela de tempo em análise.

O retorno desses dados permitirá uma segunda filtragem, possibilitando a exclusão de falsos positivos ou de números irrelevantes para a investigação, estreitando ainda mais o número de dispositivos suspeitos. Até este momento, todos os dados ainda são anônimos, isto é, os investigadores desconhecem dados pessoais dos proprietários daqueles dispositivos.

Identificados dispositivos que se mostraram relevantes para investigação, a autoridade investigadora deverá expor ao Poder Judiciário os motivos pelos quais aqueles dispositivos são relevantes para elucidar o crime e, ao final, pedirá a quebra do sigilo dos dados pessoais somente daqueles IDs específicos.

Por vezes, nessa segunda etapa ainda são requisitados mais dados anônimos e, após mais uma filtragem, só em uma terceira etapa será pedido o levantamento do sigilo e o envio dos dados pessoais dos proprietários daquelas contas.

Acatadas as razões apresentadas, a autoridade judicial requisitará ao Google informações pessoais dos proprietários daqueles dispositivos, tais como nome, número de telefone e endereços de *e-mail*.

É possível que, ao final da primeira análise, nenhum dispositivo se mostre relevante para investigação, de modo que, a rigor, nenhum sigilo terá sido quebrado, e a diligência se encerra naquela etapa.

Nos Estados Unidos, onde esse tipo de ferramenta investigativa já vem sendo usado há mais tempo, o Poder Judiciário enfrentará o pedido de reconhecimento (*United States* vs. *Chatrie*) de que o *geofence warrant* viola a Constituição estadunidense, sob o argumento de se tratar de um mandado genérico, já que os alvos não são particularizados e, consequentemente, não há demonstração de causa provável (*probable cause*) para que seja autorizada a busca (ESTADOS UNIDOS, 2019).

Okello Chatrie foi acusado de ter praticado um assalto com arma em um banco em 2019 no estado americano da Virgínia, fugindo com U$ 195.000,00. Uma câmera de segurança mostrou que o assaltante segurava um telefone celular antes de entrar no banco.

A polícia então solicitou um mandado judicial que compelisse o Google a fornecer dados anonimizados de localização de qualquer conta Google associada a dispositivos que estivessem em um raio de 150 metros do banco em uma janela de uma hora (trinta minutos antes e trinta minutos após o assalto).

O Google informou em resposta dezenove contas que estiveram dentro do raio de 150 metros durante o intervalo de tempo específico. Entre estas, uma conta chamou a atenção da polícia, pois os dados de localização a posicionavam dentro do banco no momento do assalto e corroboravam a informação de uma testemunha que disse ter visto o suspeito fora do banco antes do crime e a filmagem da câmera que mostrava a fuga após o assalto.

A polícia então requisitou ao Google informações complementares ainda anônimas de nove dentre as dezenove contas informadas anteriormente, ampliando a janela de tempo para uma hora antes e uma hora depois do crime. Identificou-se que a conta suspeita identificada na primeira análise se deslocou depois do crime até uma residência.

Pesquisando em outras bases de dados sobre aquele endereço, a polícia o vinculou a um nome individual e buscou mais informações sobre o suspeito. Por fim, foi solicitado ao Google que revelasse os dados pessoais daquela conta suspeita, cuja identidade combinou com o nome vinculado ao endereço investigado.

O caso ilustra bem a prática no tratamento dos dados obtidos pela ordem de quebra de sigilo com base em coordenadas geográficas. Ao contrário do que pode parecer, portanto, não há uma devassa na vida privada de um grande número de pessoas inocentes. Em verdade, na maior parte do tempo, trabalha-se apenas com números e códigos; somente com o avanço das investigações, é que se tem acesso a dados pessoais.

7 · PRINCÍPIO DA PRESUNÇÃO DE INOCÊNCIA E INVERSÃO DO ÔNUS DA PROVA

Existe ainda preocupação de que a quebra de sigilo de dados de pessoas vinculadas pela localização onere inocentes com o dever de provar que "apenas estavam no local errado e no momento errado". Tratar-se-ia, em outras palavras, de uma inversão do ônus da prova que, em princípio, seria da acusação.

De fato, se essa afirmativa fosse verdade, estaria sendo violado o princípio da presunção de inocência, em uma de suas vertentes, "entendido como princípio que impede a outorga de consequências jurídicas sobre o investigado ou denunciado antes do trânsito em julgado da sentença criminal" (MENDES; COELHO; BRANCO, 2009, p. 678).

De acordo com a visão moderna da doutrina, a prova tem por objeto uma hipótese sobre fatos. "O elemento e o objeto de provas não são fatos, mas crenças (aspecto doxástico) ou proposições sobre fatos (aspecto proposicional)" (DALLAGNOL, 2019, p. 122). A investigação trabalha com uma hipótese, que será confirmada ou não, a depender dos resultados das diligências que forem realizadas.

A princípio, a quebra de sigilo de dados com base em localização geográfica não tem por objeto uma hipótese que envolva algum suspeito específico. Concluindo-se pela materialidade do crime, a hipótese é de que alguém praticou uma conduta que gerou aquele resultado naturalístico. Em caso de sucesso da diligência, o resultado é a descoberta de pelo menos um suspeito. Daí começa-se a trabalhar com a hipótese investigativa propriamente dita.

O fato de apenas um indivíduo ter sido detectado na cena do crime não conduz à conclusão de que aquele é o culpado do crime, já que é possível que diversas outras pessoas também estivessem no local, embora não dispusessem de um dispositivo vinculado ao Google.

Na maioria dos crimes, o executor do fato típico está no local onde ocorreu o resultado naturalístico. Por exemplo, no caso de um homicídio a facadas, é natural que o assassino tenha estado próximo de onde o cadáver foi encontrado, seja no momento do crime, seja para deixar o cadáver no local onde se encontra.

Todavia, é evidente que nem todas as pessoas que também estiveram no mesmo local terão necessariamente alguma vinculação com o fato. Pode ser que tenham, pode ser que sejam testemunhas ou pode ser que nem sequer tenham conhecimento de que naquele local ocorreu um crime.

De início, devido ao princípio da presunção da inocência, presume-se que aquela pessoa identificada no local e horário do crime seja apenas um transeunte.

De todo modo, cabe ao órgão acusador o esforço de demonstrar as razões pelas quais entende que o(s) proprietário(s) daquele(s) dispositivo(s) pode(m) estar de alguma maneira vinculado(s) ao crime.

Concluindo-se pela vinculação, há ainda um longo caminho para que se impute a essa mesma pessoa a autoria ou participação no crime. A relevância para investigação é nada mais que a possibilidade de que o portador daquele dispositivo seja uma fonte de informação para a elucidação dos fatos e permita descobrir ou confirmar alguma linha de investigação.

É possível que se considere a comprovação da presença do suspeito no local do crime como um indício, no sentido de indício de prova, isto é, "um começo ou início de prova suficiente para formar um juízo de probabilidade do fato exigido para pronunciamentos judiciais menos gravosos do que uma condenação criminal" (DALLAGNOL, 2019, p. 128).

Nesse sentido, corrobora-se a premissa de que a quebra de sigilo servirá somente para dar início a uma linha de investigação, na qual serão empregadas medidas investigativas específicas para que se produza prova sobre a hipótese criminal aventada.

Portanto, fica claro que não há inversão do ônus da prova, já que cabe ao Estado provar que o indivíduo que estava próximo ao local e no momento dos fatos tem alguma vinculação com o crime.

Outrossim, o aspecto celeridade da persecução penal, inerente ao princípio da presunção de inocência, também deve ser considerado. A rápida solução investigativa e processual, proporcionada pelas modernas técnicas de investigação, como a exposta neste trabalho, contribui para o respeito ao princípio da presunção de inocência, visto que possibilita um desfecho rápido para o caso, afastando todo e qualquer questionamento sobre a presunção de inocência do acusado (PAULINO, 2019).

8 · UTILIDADE DA MEDIDA PARA A INVESTIGAÇÃO CRIMINAL E *FISHING EXPEDITION*

Ao se questionar sobre a utilidade de quebrar o sigilo de diversas pessoas vinculadas a um local e horário, muitos passaram a associar a quebra de sigilo telemático com base em coordenadas geográficas (*geofence warrant*) à técnica de *fishing expedition*.

O ministro do Supremo Tribunal Federal Celso de Melo classificou as *fishing expeditions* como "investigações meramente especulativas ou randômicas, de caráter exploratório, também conhecidas como diligências de prospecção" (BRASIL, 2020).

Utilizam-se ordens judiciais de busca genéricas para "jogar a rede" como expediente de pesca ou *fishing expedition* numa busca por provas, geralmente nas casas dos excluídos socialmente (LOPES JR.; ROSA, 2017).

Nesse sentido, citam-se os mandados genéricos, sem especificação subjetiva ou objetiva da medida de invasão à privacidade, a exemplo dos mandados de busca e apreensão concedidos para entrada em casas situadas em comunidades dominadas por organizações criminosas, sem que se especifiquem as casas no mandado, com base na presunção de que serão encontrados naquelas residências objetos ilícitos como drogas e (ou) armas.

Observa-se que, nesta situação, há presunção, baseada na experiência de que moradores são obrigados a esconder em suas casas armas e drogas para traficantes, de que um crime foi ou está sendo praticado naqueles imóveis.

O Google tem argumentado nas demandas judiciais sobre o assunto que a medida consiste em uma ordem exploratória, por ser baseada em meras coordenadas geográficas e atingir um sem-número de pessoas, sem qualquer individualização prévia.

Todavia, a quebra de sigilo telemático aqui estudada pressupõe uma certa individualização. Inicialmente, deve haver a definição clara do fato criminoso investigado, do local em que ocorreu – definido pelas coordenadas geográficas –, da data e do horário provável. É o que determina o art. 22, I e III, do Marco Civil da Internet quando fala de "fundados indícios da ocorrência do ilícito" e do "período ao qual se referem os registros" (BRASIL, 2014).

Geralmente, além desses dados, serão prestadas todas as informações até então conhecidas. No caso da investigação da morte da vereadora Marielle Franco, pelo que se pode depreender do que foi amplamente noticiado na mídia, a polícia tinha conhecimento de que um veículo fora utilizado na prática do crime pelos assassinos e, também, de uma filmagem em que esse veículo aparece, embora não mostre o rosto dos ocupantes. Na filmagem, era possível ver uma luz sendo emitida de um aparelho de dentro do veículo, o que indicava que o ocupante fazia uso de um dispositivo *smartphone*.

A pretensão, naquele caso, era de fazer um cruzamento de dados entre os números ID identificados no local onde se sabe que o veículo suspeito esteve antes do crime e os identificados no local em que o veículo passou após o crime. Caso a polícia identifique números ID que estiveram nos dois pontos de interesse e na janela de tempo definida, então serão solicitados dados pessoais dos usuários daquelas contas.

Portanto, no momento em que a polícia solicitou efetivamente quebra de sigilo de dados pessoais, acrescentou-se o indício de que aquelas pessoas a serem atingidas estiveram em pontos de interesse da investigação, justamente nos horários investigados.

Observa-se que, ao argumentar que a medida é desproporcional porque não oferece a mínima garantia de que levará a possíveis suspeitos do delito investigado, o Google faz um juízo de valor que caberia ao investigador, que conhece os detalhes da investigação e tem melhores condições de julgar sua utilidade para a elucidação dos fatos.

Certamente que, se a medida fosse tão inefetiva como afirma o Google, e os dados fornecidos não tivessem confiabilidade suficiente, nenhuma autoridade teria interesse em solicitar tais informações, o que não se observa na prática.

Nos Estados Unidos esse tipo de ordem judicial aumentou 1500% entre 2017 e 2018 e, de 2018 a 2019, mais de 500%. Os resultados da análise dos dados fornecidos pelo Google foram úteis na solução de um crime de homicídio em Cobb County, Georgia, de outro homicídio em Raleigh, North Carolina, de um arrombamento em Eden Prairie, Minnesota, e de um atentado a bomba em Austin, Texas (BRODY, 2020).

Parece claro que há proporcionalidade na medida, no sentido de adequação, já que, mesmo diante da possibilidade de imprecisão das localizações aferidas, as informações têm sido úteis na investigação de crimes.

Aliás, em regra, em nenhuma medida investigativa, existe garantia de que os resultados levarão aos suspeitos dos crimes. Quando se determina a busca e apreensão em algum endereço investigado, é possível que nada seja apreendido no local, o que não retira a utilidade da diligência.

Certamente que, se os requisitos de individualização do objeto de investigação não forem atendidos, a medida deverá ser indeferida pelo Poder Judiciário. Nesse sentido, a região objeto do mandado deverá ser a menor possível e demandará uma justificativa acerca das razões que levam à conclusão de que o autor do crime possa ter transitado naquela área específica. Assim, diminui-se ao máximo a possibilidade de que pessoas sem vinculação com o fato tenham seus dados de localização alcançados, ainda que de maneira anônima.

Quanto à delimitação temporal, o mandado deverá restringir a obtenção de dados de pessoas que passaram por determinado local em um determinado período de tempo. Quanto maior for o período, maior a responsabilidade de fundamentação acerca da necessidade da ampliação, tanto por parte da autoridade requerente como da autoridade que o expede.

Pode acontecer que das diligências resulte a descoberta de prática de algum outro crime diferente daquele investigado originalmente, o chamado encontro fortuito de provas. Haverá flagrante nulidade se a quebra de sigilo de dados for usada como subterfúgio para se investigar crime diverso daquele que fundamentou a medida, assim como ocorre em outros tipos de técnicas investigativas (interceptação telefônica, p. ex.). Todavia, presume-se a boa-fé dos investigadores, de modo que será necessária a demonstração do desvio de finalidade a fim de afastar esta presunção.

Em resumo, não há confusão com a técnica de *fishing expedition*, tendo em vista que, no mandado de quebra de sigilo com base em coordenadas geográficas, há certeza da ocorrência de um crime, e o fato a ser investigado é de antemão explicitado. O local do crime ou de interesse para a investigação também deverá ser precisamente definido, o que é possível atualmente graças aos modernos dispositivos que utilizam tecnologias de ponta.

9 · CONCLUSÃO

A colisão entre o direito fundamental individual à privacidade e o direito fundamental coletivo à segurança pública demanda uma solução que garanta equilíbrio e preserve o núcleo fundamental desses direitos.

Sob a perspectiva da proteção internacional dos direitos humanos, há previsão expressa de que os direitos individuais podem ceder em prol de direitos coletivos. Além disso, a Corte Interamericana de Direitos Humanos já teve a oportunidade de analisar situação parecida com a exposta neste estudo e concluiu que, embora o Estado deva proteger o direito à intimidade de seus cidadãos em frente às inovações tecnológicas, também pode usar a tecnologia em favor do direito à segurança pública.

A tecnologia tem sido usada cada vez mais para a prática de atividades criminosas. Aqueles que vivem à margem da lei se utilizam de todos as ferramentas à disposição para driblar o aparato repressivo estatal.

É contraditório cobrar do Estado postura proativa na garantia da segurança pública de seus cidadãos e, ao mesmo tempo, impedi-lo de se valer de ferramentas tecnológicas que permitam superar as inovações do mundo do crime. Sendo assim, a quebra de sigilo de dados telemáticos baseada em coordenadas geográficas de pessoas que estiveram em locais de interesse para apuração de crimes se apresenta como medida amparada pelas normas internacionais e nacionais e efetiva no combate a crimes de difícil solução.

O fato de não haver prévia delimitação dos alvos da quebra, com demonstração de indícios de autoria ou participação criminosa, não faz da medida uma ordem exploratória, já que a individualização é feita com base em outros parâmetros.

Igualmente, o simples fato de uma pessoa ter sido identificada dentro da delimitação geográfica e no período de tempo investigados não a torna automaticamente suspeita da prática do crime. Permanece sendo ônus dos órgãos de persecução penal comprovar por outros meios de prova a vinculação pessoa-fato.

Não se discorda de que a vigilância constante sobre a forma como serão utilizadas medidas investigativas invasivas é de extrema importância, a fim de se evitar o abuso estatal em detrimento de seus cidadãos, o que acontece não raramente. Todavia, não se pode engessar os órgãos persecutórios criminais no exercício de seu mister com o argumento baseado na presunção de má-fé dos investigadores.

REFERÊNCIAS

ALEXY, Robert. Minha filosofia do direito. *In*: ALEXY, Robert. *Constitucionalismo discursivo*. Org. e trad. Luís Afonso Heck. 4. ed. rev. Porto Alegre: Livraria do Advogado, 2015.

ALEXY, Robert. *Teoria dos direitos fundamentais*. Trad. Virgílio Afonso da Silva. 2. ed. São Paulo: Saraiva, 2011.

BARROSO, Luís Roberto. C*urso de direito constitucional contemporâneo*. Os conceitos fundamentais e a construção do novo modelo. 2. ed. São Paulo: Saraiva, 2010.

BRASIL. *Decreto n. 8.771, de 11 de maio de 2016*. Brasília, DF: 2016. Regulamenta a Lei n. 12.965, de 23 de abril de 2014, para tratar das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8771.htm. Acesso em: 2 jul. 2020.

BRASIL. *Lei n. 9.296, de 24 de julho de 1996*. Brasília, DF: 1996. Regulamenta o inciso XII, parte final, do art. 5º da Constituição Federal. Disponível em: http://www.planalto.gov.br/ccivil_03/Leis/L9296.htm#:~:text=Constitui%20crime%20realizar%20intercepta%C3%A7%C3%A3o%20de,a%20quatro%20anos%2C%20e%20multa. Acesso em: 2 jul. 2020.

BRASIL. *Lei n. 12.965, de 23 de abril de 2014*. Brasília, DF: 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 2 jul. 2020.

BRASIL. Supremo Tribunal Federal. *Inquérito n. 4.831/DF*. Disponível em: http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/Inq4831decisao5mai.pdf. Acesso em: 31 ago. 2020.

BRASIL. Superior Tribunal de Justiça. *Terceira Seção rejeita recurso da Google contra fornecimento de dados no caso Marielle Franco*. 26 ago. 2020. Disponível em: http://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/26082020-Terceira-Secao-rejeita-recurso-da-Google-contra-fornecimento-de-dados-no-caso-Marielle-Franco.aspx. Acesso em: 27 ago. 2020.

BRODY, Liz. Google's Geofence Warrants face a major legal challenge. *OneZero*, 2020. Disponível em: https://onezero.medium.com/googles-geofence-warrants-face-a-major-legal-challenge-ac6da1408fba. Acesso em: 31 ago. 2020.

CUNTO, Raphael de; GALIMBERTI, Larissa; LEONARDI, Marcel. Direitos dos titulares de dados pessoais. *In*: BRANCHER, Paulo Marcos Rodrigues; BEPPU, Ana Claudia (Coord.). *Proteção de dados pessoais no Brasil*: uma nova visão a partir da Lei n. 13.709/2018. Belo Horizonte: Fórum, 2019. p. 87-100.

DA SILVA, André Luiz Olivie. Os direitos humanos e o Estado "natural" de fundamentação dos direitos. *Revista Sequência*, n. 71, 2015, p. 133-154.

DALLAGNOL, Deltan Martinazzo. A visão moderna da prova indício. *In*: SALGADO, Daniel de Resende; QUEIROZ, Ronaldo Pinheiro de (Coord.). *A prova no enfrentamento à macrocriminalidade*. 3. ed. rev. atual. ampl. Salvador: JusPodivm, 2019. p. 117-140.

DWORKIN, Ronald. *Levando os direitos a sério*. Trad. Nelson 7-Boeira. São Paulo: Martins Fontes, 2002.

ESTADOS UNIDOS. United States District Court for the Eastern District of Virginia. *US v. Chatrie - Defendant's reply to motion to suppress (Geofence Warrant)*. 2019. Disponível em: https://www.eff.org/ja/document/us-v-chatrie-defendants-reply-motion-suppress-geofence-warrant. Acesso em: 2 jul. 2020.

JESUS, Damásio de; MILAGRE, José Antônio. *Manual de crimes informáticos*. São Paulo: Saraiva, 2016.

LOPES JR., Aury; ROSA, Alexandre Morais da. A ilegalidade de *fishing expedition* via mandados genéricos em "favelas". *Consultor Jurídico*, 2017. Disponível em: https://www.

conjur.com.br/2017-fev-24/limite-penal-fishing-expedition-via-mandados-genericos-favelas#_ftnref7. Acesso em: 31 ago. 2020.

MEIRELLES, Fernando de Souza. *Pesquisa anual do uso de TI nas empresas*. 31. ed. Centro de Tecnologia de Informação Aplicada (FGVcia). 2020. Disponível em: https://eaesp.fgv.br/sites/eaesp.fgv.br/files/u68/fgvcia2020pesti-resultados_0.pdf. Acesso em: 2 de ago. 2020.

MELCHIOR, Silvia Regina Barbuy. Neutralidade no direito brasileiro. *In*: DEL MASSO, Fabiano Dolenc; ABRUSIO, Juliana; FLORÊNCIO FILHO, Marco Aurélio (Coord.). *Marco civil da Internet*: Lei 12.965/2014. São Paulo: Revista dos Tribunais, 2014. p. 99-138.

MENDES, Gilmar Ferreira; COELHO, Inocêncio Mártires; BRANCO, Paulo Gustavo Gonet. *Curso de direito constitucional*. 4. ed. São Paulo: Saraiva, 2009.

OEA. Organização dos Estados Americanos. *Convenção Americana sobre Direitos Humanos,* de 22 de novembro de 1969. Disponível em: https://www.cidh.oas.org/basicos/portugues/c.convencao_americana.htm. Acesso em: 31 ago. de 2020.

OEA. Organização dos Estados Americanos. Corte Interamericana de Direitos Humanos. *Caso Escher e outros* vs. *Brasil*. Sentença de 6 de jul. de 2009.

PAULINO, Galtiênio da Cruz. *A execução provisória da pena e o princípio da presunção de inocência*. Uma análise à luz da efetividade dos direitos penal e processual penal. 2. ed. Rio de Janeiro: Lumen Juris, 2019.

PULIDO, Carlos Bernal. *El principio de proporcionalidad y los derechos fundamentales*. 4. ed. Bogotá: Universidad Externado de Colombia, 2014.

SARLET, Ingo Wolfgang. *A eficácia dos direitos fundamentais*. 7. ed. Porto Alegre: Livraria do Advogado, 2007.

SILVA, José Afonso da. *Aplicabilidade das normas constitucionais*. 2 ed. São Paulo: RT, 1982.