LIMITES E REQUISITOS DA ORDEM JUDICIAL PARA QUEBRA DE SIGILO DE DADOS ARMAZENADOS POR PROVEDOR DE SERVIÇOS NA INTERNET - Desnecessidade de individualização prévia do(s) investigado(s) e do esgotamento de outros meios de prova

Demócrito Reinaldo Filho
Desembargador do TJPE

1- Introdução

As recentes notícias sobre a resistência da Google em entregar dados para propiciar a investigação do assassinato da vereadora Marielle Franco trouxe para o debate público uma questão jurídica relevante nos dias atuais: o limite e alcance das ordens judiciais de quebra de sigilo telemático. Mais especificamente, esse caso fomentou a discussão sobre a constitucionalidade/legalidade da ordem de quebra de sigilo telemático delimitada apenas por pontos geográficos e por períodos de tempo. O assunto é muito importante por ter relação com o direito à privacidade dos indivíduos, quando confrontado com o interesse público na atividade de persecução penal e segurança pública.

O Ministério Público ingressou em juízo para obrigar a Google a fornecer os dados de todos os usuários que circularam na Via Transolímpica no dia 02 de dezembro de 2018, num intervalo de 15 minutos (entre 11:05 às 11:20). Foi nesse dia que câmeras de monitoramento de trânsito detectaram pela última vez o veículo utilizado no crime. A intenção dos promotores era que, com os dados requisitados, pudesse ser identificado quem estava

utilizando o veículo¹. Apesar de a Justiça do RJ ter autorizado a quebra do sigilo telemático, a empresa recorreu da decisão ao STJ².

A Google justificou a recusa com a tese de que estava protegendo a privacidade dos seus usuários, argumentando que a ordem judicial para quebra de dados de uma maneira "genérica", sem especificar as pessoas objeto da investigação, não tem respaldo constitucional ou legal.

Esse caso não é o único que está sendo discutido nas cortes brasileiras. São inúmeros os processos, em diversos Estados, em que a Google aparece contestando decisões de juízes que determinam a entrega de dados de uma maneira "genérica", com a quebra de sigilo telemático apenas com base em coordenadas geográficas e limites temporais³. Não somente a Google vem contestando com insistência esse tipo de requisição judicial, mas também outras empresas de tecnologia e provedores de serviços na Internet vêm se negando a fornecer os dados que armazenam, ainda que para fins de investigação criminal ou instrução processual. Essa discussão sobre a amplitude e requisitos da ordem judicial para quebra do sigilo telemático também está na pauta de cortes judiciárias em diversos outros países.

¹ Ver reportagem publicada no site Globo.com, em 30.01.20, acessível em: <https://oglobo.globo.com/rio/mp-do-rio-briga-na-justica-com-google-para-identificar-ocupantes-do-carro-usado-no-assassinato-de-marielle-24205735>

² Ver notícia publicada no site Conjur, em 31.01.20, acessível em: <https://www.conjur.com.br/2020-jan-31/google-recorre-stj-quebra-sigilo-marielle>

³ Na condição de integrante da 2^a. Turma da Câmara Regional de Caruaru (do Tribunal de Justiça de PE), tivemos oportunidade de julgar caso idêntico, em que também houve resistência da Google ao fornecimento de dados requisitados com a finalidade de investigação de um homicídio ocorrido na cidade de Jupi-PE. Os argumentos da Google para não fornecer os dados solicitados foram exatamente os mesmos com que recusou o cumprimento do mandado para entrega de dados no caso da vereadora Marielle.

Devido à importância, repercussão e atualidade do tema, resolvemos realizar um estudo sobre as requisições judiciais de dados com base apenas em coordenadas geográficas ou limites temporais. No presente trabalho, demonstramos que as ordens judiciais de quebra de sigilo de dados dirigidas aos provedores têm previsão legal, não possuem caráter “exploratório” e não produzem repercussão negativa ou desarrazoada sobre a privacidade de terceiros inocentes. A legislação já estabelece os requisitos para que essas requisições sejam adotadas, bem como prevê salvaguardas e medidas de segurança informacional que podem ser adotadas para o procedimento não exceder sua finalidade, como demonstramos adiante.

2- Argumentos dos provedores contra as requisições judiciais para entrega dos dados

Embora não tendo lido os autos do processo movido contra a Google para requisição de dados na investigação do caso Marielle Franco, na condição de integrante da 2^a. Turma da Câmara Regional de Caruaru (do Tribunal de Justiça de PE) tive oportunidade de decidir caso idêntico, em que também houve resistência da empresa ao fornecimento de dados requisitados com a finalidade de investigação de um homicídio ocorrido na cidade de Jupi-PE⁴. Do que se extrai das notícias veiculadas na imprensa, os argumentos da Google para não fornecer os dados solicitados no caso Marielle devem ter sido exatamente os mesmos com que recusou o cumprimento do mandado para

⁴ Mandado de Segurança, proc. n. 0547762-5 (NPU 0000343-50.2020.8.17.0000). Impetrante: Google Brasil Internet Ltda. Autoridade coatora: Juiz de Direito da Comarca de Jupi-PE. Relator: Desembargador Demócrito Reinaldo Filho. Órgão julgador: 2^a. Turma da Câmara Regional de Caruaru (TJPE).

entrega de dados no caso que decidi. Os argumentos jurídicos da Google são de certa forma os que vêm sendo utilizados por outras empresas de tecnologia e provedores de serviços na Internet que se negam a fornecer dados para fins de investigação ou instrução processual. Assim, o relato das circunstâncias do caso que decidi, com a explicação dos fundamentos utilizados pela Google, servirá para situar o leitor não só sobre o que ocorreu naquele caso bem como para trazer para um debate mais amplo a questão dos limites das ordens de quebra de sigilo telemático.

A Google Brasil Internet Ltda. impetrou **mandado de segurança** contra ato do Juiz da Vara Única da Comarca de Jupi/PE, que determinara a quebra de sigilo informacional com a finalidade de apuração de crime de homicídio. De forma específica, a decisão atacada determinou a "quebra do sigilo telemático dos usuários de telefonia celular cujos aparelhos, no dia 06 de maio de 2018, no período compreendido entre as 05:00 e 08:00, encontravam-se no raio de até 200 metros" de certas localidades (como a residência da vítima, o ponto provável de início da perseguição, o local onde foi praticado o homicídio e o ponto provável da fuga). A ordem determinou ainda que a Google fornecesse "a relação dos números identificadores (N-ID) dos aparelhos celulares, que dentro do período de tempo acima mencionado, estejam dentro do raio de até 200 (duzentos) metros de quaisquer coordenadas constantes da tabela acima", ressaltando ainda que a "relação deve vir acompanhada de todos os dados de localização, sejam derivados do Sistema de Posicionamento Global (GPS), triangulação de célula em estação rádio-base, informações de medidas precisas como percurso de tempo (*time advance*) ou PCMD (*Per Call Measurement Data*),

localização de *wi-fi*, incluindo coordenadas GPS, raio estimado, e os horários de todos os registros de localização abarcados pela delimitação temporal e espacial acima mencionada”.

A Google alegou que a quebra do sigilo telemático de um conjunto não identificado de pessoas, que sequer ostentam a condição de suspeitos, unidas tão somente pela circunstância de terem transitado por certas coordenadas geográficas no Município de Jupi/PE em certo lapso de tempo, não tem previsão constitucional ou base legal. Aduziu que qualquer medida de quebra de sigilo informacional pressupõe necessariamente a individualização dos alvos da ordem, isto é, a especificação das pessoas suspeitas e que são objeto da investigação, nos termos do que dispõem o art. 2º. da Lei n. 9.296/96, a Resolução CNJ n. 59/2008, o art. 22 do “Marco Civil da Internet do Brasil” (Lei n. 12.965/14) e o art. 11 do Decreto Federal n. 8.771/2016. Afirmou que “inexiste autorização legal para a determinação de quebra de sigilo de uma gama de pessoas não individualizadas, a partir do mero fornecimento de coordenadas geográficas referentes ao local de ocorrência de certo crime”, pois a ordem jurídica brasileira não prevê, como medida investigativa, “a exploração de plataformas de empresas de internet para fornecimento de dossiês de informações de usuários indeterminados”, sem a delimitação de salvaguardas para as prerrogativas individuais dos cidadãos. A ordem constitucional não permite que se afaste a privacidade de um grande número de indivíduos apenas por terem estado em determinado local em dado momento. Nesse aspecto, sustentou, a medida impugnada constitui uma violação ao princípio da legalidade (art. 5º., II, e 37, *caput*, da CF), pois teria que estar prevista em lei. “Quebras de sigilo são admitidas apenas em face

daqueles contra os quais existam indícios de envolvimento em atividade ilícita". Ainda quando movido pelo interesse de investigar crimes, o Estado não pode atuar fora da legalidade. Se o meio de prova decorrente do uso de novos recursos tecnológicos ainda não possui regramento em lei, a prova recolhida é ilícita, concluiu.

Argumentou também que a decisão atacada não continha fundamentação adequada, pois não é suficiente a mera alegação da finalidade de elucidação de crimes, sendo imprescindível que o magistrado justifique a necessidade da restrição a direitos individuais. Por fim, argumentou que a ordem impugnada feria o princípio da proporcionalidade, pois não se tem garantia de que as informações requisitadas levem aos autores do delito investigado, em razão da imprecisão dos dados. Diversos fatores como meio de conexão, qualidade do sinal, horário e local de captação, a geografia do lugar, o modelo de dispositivo (aparelho celular) "geram aleatoriedade na coleta dos dados de localização e podem tornar a produção dos dados requisitados severamente randômica", daí que "podem deixar de indicar usuários que estiveram no local ou mesmo apontar pessoas que não estiveram, com potencial de gerar falsos indícios". Essas circunstâncias retiram a utilidade da medida e afastam a confiabilidade desse meio de obtenção de prova. Para ser válida, a restrição a um direito fundamental necessita ser capaz de satisfazer o fim a que se destina. É preciso que fique demonstrada a adequação da medida de quebra do sigilo informacional à finalidade pretendida. Sustentou que, além de ser apta a produzir os objetivos pretendidos, a medida restritiva tem que estar baseada numa situação de necessidade, ou seja, é preciso que fique demonstrado a inexistência de outras medidas menos gravosas e igualmente idôneas à produção do resultado

pretendido. Alegou existirem outras medidas alternativas e menos invasivas, capazes de levar à individualização dos suspeitos. Afirmou que o art. 2º. da Lei n. 9.296/96 exige, para a quebra de sigilo telefônico e de dados telemáticos, não somente a demonstração de indícios de autoria ou participação da pessoa investigada, mas também de que a prova seja necessária, não havendo outros meios menos invasivos. A Resolução n. 59/2008 do CNJ, que disciplina a interceptação telefônica e telemática, reforça a necessidade na ordem judicial de quebra de sigilo da indicação de indícios razoáveis de autoria ou participação dos alvos na infração criminal investigada. Da mesma forma, o art. 22 do "Marco Civil da Internet" (Lei n. 12.965/14) só admite a quebra do sigilo de registros de conexão e de acesso a aplicações mediante a justificativa motivada dos dados requeridos. O Decreto Federal n. 8.771/16 também veda "pedidos genéricos ou inespecíficos" de dados cadastrais, determinando que "devem especificar os indivíduos cujos dados estão sendo requeridos e as informações desejadas" (art. 11, § 3º.). Finalizou argumentando que a decisão impugnada não atende o requisito da proporcionalidade em sentido estrito, pois provoca dano colateral exagerado consistente na quebra do sigilo de inocentes. A amplitude e a extensão da medida, que afeta uma área muito grande e exige a entrega de uma massa enorme de informações, revelando o seu potencial invasivo, sem garantias de assegurar a eficiência da investigação criminal, gera mais prejuízos do que benefícios sociais, o que por si só denota a desproporcionalidade da ordem judicial.

Justificou que "não pode haver quebra de sigilo com base apenas na localidade e no lapso de tempo em que teria ocorrido o crime". Ordens "genéricas" e "exploratórias" de quebra de sigilo informacional, que

produzem uma devassa indiscriminada na esfera da intimidade das pessoas, são inconstitucionais. Defendeu que não pode ser obrigada a cumprir uma ordem com essa amplitude, pois isso implicaria em realizar "uma varredura generalizada em suas plataformas". A ordem "busca transformar cada aparelho celular em uma ferramenta para vigilância absoluta e indiscriminada, instaurando autêntico Estado policial". Sem conter a individualização das pessoas afetadas, a ordem equivale a um "monitoramento preventivo ou aleatório dos cidadãos", violando a garantia constitucional da privacidade individual (art. 5º., X, da CF) e a regra protetora do sigilo das comunicações (art. 5º., XII). Ao Estado não é conferido o poder absoluto de vasculhar, sem quaisquer limitações, registros sigilosos e alheios, concluiu.

3- Questão da (i)legitimidade do provedor destinatário da ordem de quebra do sigilo informacional para defender a privacidade dos seus usuários

Uma questão preliminar, que antecede a discussão sobre a constitucionalidade/legalidade da ordem de quebra de sigilo telemático delimitada apenas por limites geográficos e de tempo, reside em se saber se o provedor de serviços na Internet ou qualquer empresa de tecnologia tem *legitimidade* para se opor ao cumprimento da ordem alegando a defesa da privacidade de seus usuários, sabendo-se que ninguém pode defender direitos alheios.

Para postular em juízo é necessário ter *interesse* e *legitimidade* (art. 17 do CPC), não podendo ninguém pleitear direito alheio em nome próprio, salvo quando autorizado por lei (art. 18). Embora o provedor figure como destinatário da ordem judicial, não aponta

qualquer interesse ou direito de sua titularidade que possa ser atingido pela quebra do sigilo telemático. Em regra, nos processos judiciais movidos pelos provedores para se contrapor a uma requisição para entrega de dados, toda a fundamentação jurídica é baseada na alegada defesa de direitos dos usuários dos seus serviços ou mesmo de terceiros que possam ser atingidos pela ordem judicial. Para demonstrar seu *interesse* em impugnar a decisão, o provedor tem que reputar ilegal a ordem com base em eventual direito seu de não prestar as informações solicitadas. O provedor pode, por exemplo, invocar a alegativa de que a ordem impugnada fere o seu dever de guarda dos dados ou que tem potencial de revelar algum segredo industrial. O que não pode é contestar a ordem judicial pretendendo a defesa da privacidade de terceiros, por não ser *representante* deles e nem lhe ser conferida pela lei a qualidade de *substituto processual*. Qualquer pessoa que se sentir lesada, por entender que a ordem alcança sua órbita de interesses, pode individualmente fazer a defesa de eventuais direitos lesados.

Em outros países existe esse mesmo debate, em torno da *legitimidade* de empresas de tecnologia para defender interesses de seus usuários relacionados à privacidade individual. Em dezembro de 2015, o Tribunal de Apelações do Estado de Nova Iorque (nos EUA) decidiu que o Facebook não tinha *legitimidade* para contraditar uma ordem judicial que requisitava informações sobre as contas de 381 usuários, para possibilitar a investigação de fraude cometida contra a previdência social. O Facebook alegou justamente a amplitude da ordem e seu efeito sobre a privacidade dos seus usuários, protegida constitucionalmente. Por 5 votos a 1, a Corte decidiu que somente os alvos da investigação poderiam se insurgir

contra a ordem e que o Facebook não tinha *legitimidade* para defender interesses de terceiros⁵.

4- Os provedores de serviços na Internet não são os titulares e não podem pretender um monopólio sobre os dados que coletam e armazenam

Como já se disse, estamos diante de importante questão que as cortes brasileiras começam a ser chamadas a decidir: qual o limite e os requisitos da ordem judicial de quebra do sigilo de dados sob a guarda de provedor de Internet.

A definição de parâmetros nesse tema ganha especial relevância diante do desenvolvimento das tecnologias, sabendo-se que nos dias atuais a informação é processada e tratada em grande volume, variedade e velocidade, formando imensos conjuntos de dados que são em seguida estruturados, armazenados e analisados por meio de técnicas computacionais, fenômeno definido pelo conceito de *Big Data*. Diversas ferramentas e equipamentos, conectados à rede mundial de comunicação, coletam e processam informações pessoais.

Essas informações não podem permanecer em poder exclusivo das empresas que, para desempenho de suas atividades, realizam a coleta e tratamento dos dados pessoais. Elas apenas guardam e processam as informações de terceiros para o desenvolvimento de atividades legítimas, quando autorizadas pela lei ou mediante consentimento do titular dos dados. O fato de processar informações de terceiros, não torna a empresa responsável por essa

⁵ O caso foi catalogado como *In re: 381 Search Warrants Directed to Facebook Inc, New York State Court of Appeals, No. 16*. Ver notícia publicada em 04.04.17 sobre o julgamento, acessível em: <http://www.reuters.com/article/us-facebook-new-york-idUSKBN1762MY>.

operação titular dos dados coletados. O operador ou controlador de um sistema informatizado que realiza o tratamento de dados pessoais não adquire a titularidade desses dados e nem tem o controle absoluto sobre eles. A guarda ou utilização dos dados é realizada apenas para atingir a finalidade da operação e pelo tempo necessário para se alcançar o objetivo pretendido. O titular continua sendo a pessoa natural a quem se referem os dados pessoais objeto do tratamento.

Em regra, somente o titular dos dados tem o direito de ter acesso a eles, para pedir sua correção, eliminação ou transferência (portabilidade) a outro prestador de serviços. Exigências de ordem social e razões fundadas no interesse público, contudo, podem justificar a entrega dos dados pessoais coletados pelos sistemas informatizados de empresas privadas às autoridades públicas. Diversas situações, que evidenciem a necessidade de se proteger o direito à vida, saúde e segurança dos cidadãos concorrem como causa justificadora da quebra do sigilo das informações pessoais que estejam em poder de empresas de tecnologia. A necessidade de viabilizar uma investigação criminal ou a instrução de um processo judicial é um exemplo de situação excepcional que pode autorizar a quebra do sigilo informacional.

E cada vez mais as autoridades públicas vão necessitar dos dados coletados e armazenados por empresas de tecnologia, para fins de investigação criminal ou instrução processual. A cada dia se inventam novos aparelhos e objetos com diversas funcionalidades, conectados à rede Internet, capazes de coletar e processar dados. Não somente sites, motores de busca na Internet e câmeras de vigilância são capazes de colher e tratar dados. Novos *gadgets* aparecem no mercado a cada dia com potencial

de coleta de dados, integrados ao cotidiano das pessoas em ambientes de trabalho, nos veículos e em residências. Sistemas operacionais de veículos⁶, campanhas, termostatos, aparelhos "vestíveis" (*weareables*), assistentes pessoais⁷ e aplicativos em geral gravam conversas, filmam cenas e recolhem dados sobre todos os aspectos das vidas das pessoas, ficando armazenados em servidores das empresas fabricantes desses equipamentos inteligentes. Em breve, praticamente todos os eletrodomésticos que equipam residências e escritórios vão estar interligados à rede Internet (*IoT*⁸), funcionando mediante a coleta e transmissão de dados. Os dados processados por esses aparelhos e armazenados em servidores podem servir como meio de prova e valioso recurso na investigação e repressão a crimes.

Ocorre que as empresas de tecnologia e provedores de aplicações na Internet têm se recusado a fornecer os dados que armazenam às autoridades policiais, ministeriais e judiciárias, objetando toda ordem de argumentos e colocando diversos empecilhos à entrega das informações, com o intuito de fugir ao império da lei nacional e em desabrida afronta à soberania digital do nosso país.

Os argumentos utilizados para não cumprir decisões judiciais de quebra de sigilo informacional são diversos. Para ser furtar ao cumprimento de ordens judiciais, empresas de tecnologia e provedores de serviços na Internet já alegaram dificuldades técnicas para acesso aos dados da comunicação em aplicativo com criptografia⁹,

⁶ Como o *Apple Car Play*, da Apple, e o *Android Auto*, da Alphabet.

⁷ Como o *Alexa*, da Amazon, e o *Google Home*, da Alphabet.

⁸ Sigla para *Internet of Things* (Internet das Coisas, em português),

⁹ Não custa recordar o caso da resistência do Facebook, que controla o aplicativo de mensagens instantâneas *Whatsapp*, à decisão da juíza da 2ª. Vara Criminal da Comarca de Duque de Caxias-RJ, que ordenou o bloqueio do aplicativo em todo país, por ter a empresa se negado a

que os dados estavam hospedados em servidor situado em outro país¹⁰, que o serviço ou aplicação era operado pela matriz americana (e, portanto, não submetida à jurisdição nacional)¹¹ e que a abrangência da quebra do sigilo viola princípios constitucionais ou que não tem base legal.

A resistência ao cumprimento de decisões judiciais já resultou em bloqueio de sites e aplicativos, imposição de multas¹² e até prisão de executivos¹³. As

atender requisição para entrega de dados necessários à investigação de crimes graves praticados por uma quadrilha que atuava no município, alegando que não tinha meios técnicos para quebrar a *criptografia* das mensagens enviadas por meio do aplicativo. Ver, a respeito dessa polêmica, artigo que escrevemos na época dos fatos, sob o título "*CODE IS NOT LAW: a empresa que controla o Whatsapp precisa se submeter ao império da lei nacional*", publicado no site *Jus Navigandi* e acessível em: <https://jus.com.br/artigos/50898/code-is-not-law-a-empresa-que-controla-o-whatsapp-precisa-se-submeter-ao-imperio-das-leis-nacionais>

¹⁰ A própria Google também de há muito vem se recusando a cumprir decisões judiciais, pelos mais diversos fundamentos. Em abril de 2014, ingressou com mandado de segurança no TJRN para não cumprir a decisão do Juiz da Comarca de Caraúbas, que determinara a entrega de mensagens eletrônicas (*e-mails*) trocadas por investigados de crime grave. Baseou sua recusa na alegação de que os arquivos solicitados encontravam-se armazenados em servidor nos EUA e que somente poderia entregá-los com ordem emanada de juiz norte-americano. O mandado de segurança foi negado pelo TJRN. Ver notícia publicada no site *Convergência Digital*, em 28.04.14, acessível em: <http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?infoid=36604&sid=16#.U178WIFdUZ4>

¹¹ O Facebook foi condenado a pagar uma multa de R\$ 3,96 milhões, por descumprir diversas ordens judiciais, pelo Juiz da 5ª Vara Federal de Guarulhos. Em uma das decisões, a Justiça Federal havia pedido quebra de sigilo de usuários da rede social, em investigações relacionadas a uma quadrilha que importava e distribuía anabolizantes sem licença da Anvisa. Em janeiro de 2017, a empresa recorreu da multa ao Tribunal Regional Federal da 3ª Região, e perdeu. No final daquele ano, o STJ decidiu que as multas eram válidas. O argumento do Facebook é que seu serviço de rede social é operado pela *Facebook Inc.*, sua matriz americana. Todas as instâncias da Justiça consideraram que essa justificativa era apenas uma tentativa de se "esquivar ao cumprimento das ordens". Ver notícia publicada em 19.02.18, acessível em: <https://noticias.r7.com/tecnologia-e-ciencia/facebook-e-multado-em-r-396-mi-por-descumprir-ordem-judicial-19022018>

¹² A Justiça Federal em Mato Grosso aplicou multa e bloqueou quantia expressiva do Facebook também por ter se recusado a interceptar mensagens de usuários do *Whatsapp*, sob a mesma alegação de que a tecnologia adotada para codificar as mensagens (criptografia) impede de copiar o conteúdo das comunicações realizadas por meio desse aplicativo. Ver notícia publicada no site *G1*, em 29.09.16, acessível em: <http://g1.globo.com/mato-grosso/noticia/2016/09/juiz-federal-de-mt-determina-bloqueio-de-r-69-milhoes-do-facebook.html>

companhias de tecnologia têm se negado a atender determinações de autoridades judiciárias não somente aqui¹⁴ mas em outros países¹⁵.

Esse comportamento dos provedores de serviços na Internet e das empresas de tecnologia em geral revela que outros interesses podem estar escondidos por trás da alegada defesa da privacidade dos usuários. As mesmas empresas que vivem bisbilhotando a vida das pessoas, monitorando seus passos, seus gostos e hábitos, e coletando cada vez mais dados pessoais, se opõem a que as autoridades judiciárias tenham acesso a esses mesmos dados, ainda que para fins de se apurar crimes graves, ou seja, para finalidade de acentuado interesse público e em benefício da sociedade, a quem interessa a elucidação de crimes e a persecução penal. Quando se opõem ao cumprimento dessas ordens, alegam que estão apenas defendendo a privacidade das pessoas, mas é fácil entrever que na verdade estão defendendo os próprios interesses. As empresas de tecnologia querem ter o monopólio dos dados, concentrando a grande massa de informações que reúnem sobre os usuários

¹³ O Vice-Presidente do Facebook no Brasil terminou sendo processado por desobediência pela Justiça de São Paulo por ter se recusado a interceptar mensagens enviadas por meio do aplicativo *Messenger*. Ver notícia publicada no site *Convergência Digital*, em 12.04.17, acessível em:

<http://www.convergenciadigital.com.br/cgi/cgilua.exe/sys/start.htm?UseActiveTemplate=site&infpid=44962&sid=4>

¹⁴ A *Amazon* negou-se a apresentar registros de áudio armazenados em seu servidor e capturados pelo equipamento *Echo* (um *smart speaker* que funciona acoplado ao *Alexa*, assistente pessoal dotado de inteligência artificial) a pretexto de proteger a privacidade dos usuários, embora os dados fossem necessários para a solução de um caso de homicídio. Ver notícia publicada no site especializado em assuntos de tecnologia *Arsthecnica*, em 23.02.17, acessível em: <https://arstechnica.com/tech-policy/2017/02/amazon-wont-disclose-if-alexa-witnessed-a-murder/>

¹⁵ Para desvendar um caso envolvendo uma fraude financeira, policiais da cidade de Edina (no Estado de Minnesota, EUA) obtiveram mandado judicial para forçar a *Google* a revelar quem havia pesquisado no seu motor de busca o nome da vítima, num período de pouco mais de um mês e dentro de uma área de 15 milhas quadradas. Ver notícia publicada no site especializado em assuntos de tecnologia *Arsthecnica*, em 17.03.17, acessível em: <https://arstechnica.com/tech-policy/2017/03/judge-oks-warrant-to-reveal-who-searched-a-fraud-victims-name-on-google/>

para suas únicas finalidades privadas e comerciais. **Informação é poder.** Quem tem o controle sobre os dados, controla a vida das pessoas a quem se referem. Por outro lado, as empresas querem evitar os custos relacionados com o atendimento às requisições judiciais. Para atender à demanda judicial por informações, precisam alocar recursos humanos e materiais para essa tarefa, o que representa gasto adicional no orçamento. O que elas prefeririam, certamente, era vender esses dados ao Poder Público, como, aliás, já estão fazendo nos Estados Unidos¹⁶. Nesse país, a Google já está cobrando para atender as solicitações feitas por autoridades policiais para entrega ou preservação de dados¹⁷. A empresa diz que decidiu cobrar para compensar o custo com a produção das informações e inclusive já publicou uma tabela com os preços cobrados¹⁸.

5- Leis diferentes (Lei n. 9.296/96 e Lei n. 12.965/14) disciplinam com requisitos diversos o procedimento da requisição judicial para entrega de dados armazenados pelo

¹⁶ O Governo americano, segundo reportagem do jornal *Wall Street Journal*, está comprando dados de localização emitidos pelos aparelhos celulares, para facilitar o controle sobre a imigração e as fronteiras. Através desses dados, o Governo está conseguindo localizar e prender imigrantes ilegais. Os dados são comprados legalmente de empresas que trabalham com marketing digital. Ver reportagem publicada em 07.02.20, acessível em: <https://www.wsj.com/articles/federal-agencies-use-cellphone-location-data-for-immigration-enforcement-11581078600>

¹⁷ Alguns tipos de dados podem ser entregues diretamente às autoridades policiais, sem necessidade de mandado judicial, como por exemplo algumas categorias de dados anonimizados, metadados e dados de geolocalização de aparelhos móveis (celulares). Já dados que revelam o conteúdo de comunicações e os que permitem identificar as pessoas a que se referem (dados pessoais) só podem ser fornecidos mediante ordem judicial. Mas em relação a esses últimos as autoridades policiais podem requerer ao provedor que sejam preservados, enquanto conseguem obter autorização judicial para acesso a eles.

¹⁸ Nos EUA leis permitem que empresas cobrem um valor como forma de ressarcimento pelos custos do atendimento de requisições legais. Ver reportagem publicada pelo site Olhar Digital, em 27.01.20, acessível em: <https://olhardigital.com.br/noticia/google-define-precos-para-entregar-dados-de-usuarios-as-autoridades/95857>

provedor e o da interceptação das comunicações (telefônica, telegráfica ou telemática)

A resistência dos provedores ao cumprimento de decisões judiciais de quebra de sigilo telemático não prospera e deixa entrever que constitui mera estratégia das empresas a fim de procrastinar a entrega dos dados. Isso fica claro diante da fragilidade dos fundamentos jurídicos e argumentos, alguns inconsistentes de um ponto de vista lógico. A debilidade dos fundamentos está presente inclusive na confusão que é feita sobre conceitos técnico-jurídicos.

O caso da ação (de mandado de segurança) ajuizada pela Google contra a decisão do Juiz da Comarca de Jupi(PE)¹⁹, que ordenou a entrega de dados armazenados pela empresa para possibilitar a investigação de um homicídio, concorre para sedimentar essa visão do problema.

Como ponto central da ação mandamental a Google arrazoou que a ordem para quebra do sigilo informacional (sigilo de dados) tem que, obrigatoriamente, indicar os "alvos" da investigação, ou seja, o magistrado precisa identificar previamente na decisão as pessoas suspeitas e que são objeto da investigação. Isso é uma exigência contida no art. 2º. da Lei n. 9.296/96, na Resolução CNJ n. 59/2008, no art. 22 do "Marco Civil da Internet do Brasil" (Lei n. 12.965/14) e no art. 11 do Decreto Federal n. 8.771/2016, segundo a Google. Aduziu que não existe previsão no ordenamento jurídico brasileiro para "quebra de sigilo de uma gama de pessoas não individualizadas, a partir do mero fornecimento de coordenadas geográficas referentes ao local de ocorrência

¹⁹ Mandado de Segurança, proc. n. 0547762-5 (NPU 0000343-50.2020.8.17.0000).

de certo crime” e de um lapso de tempo estipulado aleatoriamente.

O primeiro erro que a Google fez foi combater a ordem de quebra do sigilo informacional com base em dispositivos legais e constitucionais que regulamentam a interceptação das comunicações. A empresa fez uma confusão entre conceitos técnico-jurídicos, tratando a ordem para apresentação de arquivos digitais de registros de conexão e acesso a aplicações de Internet, e eventuais dados pessoais a eles vinculados, como se fosse ordem para a interceptação do fluxo de comunicações de dados. Ao se insurgir contra a ordem emitida pelo magistrado do primeiro grau com fundamento no inc. XII do art. 5º. da CF, na Lei n. 9.296/96 e na Resolução CNJ n. 59/2008, a Google elencou requisitos só aplicáveis ao ato de interceptação da comunicação (telefônica, telegráfica ou telemática), no que reside o equívoco. “Interceptar é interromper o curso originário, impedir a passagem, sendo que na lei tem o sentido de captar a comunicação, conhecer seu conteúdo. Interceptar é ter contato com o teor da comunicação, não impedindo que ela chegue ao seu destinatário”²⁰.

O inc. XII do art. 5º. da CF garante a inviolabilidade do **sigilo da correspondência e das comunicações**, abrangendo a comunicação telemática²¹, somente admitindo uma única exceção a esse direito: a interceptação mediante prévia autorização judicial e desde que se destine à investigação criminal ou instrução

²⁰ ARAÚJO DE CASTRO. Carla Rodrigues. Crimes de Informática e seus aspectos processuais. Rio de Janeiro. Editora Lúmen Júris, 2001, págs. 101 e 102.

²¹ “A telemática é uma ciência que trata da manipulação de dados e informações, conjugando o computador, sistemas de informática, com os meios de comunicação, telefônicas ou não. Assim, qualquer comunicação feita através de sistema de informática é protegida pela lei; a título de exemplo, citamos as comunicações feitas na Internet.” Ob. cit.

processual penal²². Mesmo admitindo exceção ao sigilo das comunicações, a Constituição adotou regras para que a interceptação não se faça com abusos. Além de exigir prévia autorização judicial, o texto constitucional somente admite a quebra do sigilo das comunicações para duas finalidades: investigação criminal ou instrução processual penal. Ainda por cima, o procedimento para a interceptação deve obedecer às hipóteses e forma estabelecidas em lei. A Lei n. 9.296, de 24 de julho de 1996, regulamentou o inc. XII, parte final do art. 5º. da Constituição Federal, estabelecendo requisitos formais e procedimentais para a interceptação judicial das comunicações interpessoais. Dentre os requisitos, a Lei em questão exige indícios razoáveis da autoria ou da participação em infração penal. Assim, alguma prova da autoria, que identifique previamente o sujeito "alvo" da medida, deve embasar a decisão que determina a interceptação²³. O segundo requisito refere-se à ausência de outro modo para demonstrar o fato apurado. A interceptação só será concedida quando for o único meio para provar a conduta delituosa. Por fim, é cabível apenas nos crimes punidos com reclusão²⁴.

²² O dispositivo citado tem a seguinte redação:

"é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal".

²³ Ainda assim, a exigência de que seja feita a indicação e qualificação dos investigados não é absoluta, pois a própria Lei prevê a dispensa desse requisito no caso de "impossibilidade manifesta, devidamente justificada" (§ único do art. 2º.).

²⁴ Os requisitos para a interceptação das comunicações estão descritos no art. 2º. da Lei 9.296/96, que tem a seguinte redação:

"Art. 2º Não será admitida a interceptação de comunicações telefônicas quando ocorrer qualquer das seguintes hipóteses:

I - não houver indícios razoáveis da autoria ou participação em infração penal;

II - a prova puder ser feita por outros meios disponíveis;

III - o fato investigado constituir infração penal punida, no máximo, com pena de detenção."

A Lei n. 9.296/96 e a Resolução CNJ n. 59/2008 não têm aplicação quando se trata de proceder a uma requisição de dados pessoais que uma operadora de telefonia ou um provedor de serviços de Internet tenha armazenado em seus servidores e sistemas informatizados. Isso porque, como se disse, essas normas regulam o procedimento para a interceptação das comunicações (telefônicas, telegráficas ou de dados). A interceptação, como também já explicado, compreende a captação da conversa alheia, e ocorre no momento real e imediato em que se estabelece a comunicação, por intermédio de gravações ou escutas. Já a quebra do sigilo de dados corresponde à obtenção de registros informacionais existentes na empresa, sobre ligações já realizadas²⁵ ou dados já coletados.

As restrições formais e procedimentais elencadas na Lei n. 9.296/96 (e na Resolução CNJ n. 59/2008) não são aplicáveis por extensão ou analogia à quebra de sigilo de dados, sobretudo quando a ordem é dirigida a um provedor de serviço de conexão ou aplicações de Internet. Isso porque existe lei específica, disciplinando a requisição judicial de dados pessoais em poder dos provedores, para fins de instrução processual. Trata-se da Lei n. 12.965, de 23 de abril de 2014 ("Marco Civil da Internet"), que não elenca, dentre os requisitos que estabelece para a quebra do sigilo informacional, que a ordem judicial especifique previamente as pessoas objeto da investigação ou que a prova da infração (ou da autoria) possa ser realizada por outros meios. Muito pelo contrário, o parágrafo 1º. do art. 10 da Lei n. 12.965/14 estabelece que o propósito primário da quebra do sigilo informacional pode ser justamente a descoberta da autoria de crimes.

²⁵ Uma empresa operadora de telefonia, por exemplo, pode preservar uma série de dados sobre ligações já realizadas, como dados cadastrais do assinante, data da chamada, horário, número do telefone chamado, duração do uso, valor da chamada etc.

Observe-se quando o citado dispositivo menciona que os registros de conexão²⁶ e de acesso a aplicações²⁷ podem, **associados a outros dados pessoais** coletados pelos provedores, ser objeto de requisição judicial para identificação dos usuários desses serviços:

“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.”
(grifamos)

Como se observa, o objetivo primacial da quebra do sigilo de dados é a identificação do usuário do

²⁶ Nos termos do inc. VI do art. 5º. da Lei n. 12.965/14, **registro de conexão** é “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”.

²⁷ Nos termos do inc. VII do art. 5º. da Lei n. 12.965/14, **registro de acesso a aplicações de internet** é “o conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP”.

serviço ou terminal. A quebra do sigilo informacional tem justamente a finalidade de proporcionar a descoberta da identidade de quem fez uso do serviço ou acessou um determinado terminal, em algum momento e em certa localidade.

A Seção IV do Capítulo III da Lei n. 12.965/14, que cuida especificamente da "Requisição Judicial de Registros", não contém nenhum dispositivo que exija a indicação ou qualquer elemento individualizador, na decisão judicial, da pessoa que ostenta a condição de suspeito e que está sendo investigada. Para a quebra do sigilo de dados, a Lei não requer os mesmos requisitos que são exigidos para a interceptação telefônica ou telemática. A interceptação, como antes explicado, consiste em captar o fluxo da comunicação interpessoal, no momento em que ela se estabelece; já a quebra do sigilo informacional envolve a requisição de dados pessoais armazenados pelo provedor de serviço de Internet. Para a quebra do sigilo de dados, os requisitos traçados na Lei 12.965/14 são diferentes, conforme consta do seu art. 22, *verbis*:

"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."**

Constata-se, portanto, que para o Juiz requisitar dados pessoais armazenados por provedor de serviços de Internet, basta fundamentar sua decisão com os seguintes elementos: a) indícios da ocorrência do ilícito; b) justificativa da utilidade da requisição; e c) período ao qual se referem os registros. Não é necessário que o magistrado fundamente a requisição com indicação da(s) pessoa(s) alvo(s) da investigação, nem tampouco que justifique a indispensabilidade da medida requestada, ou seja, que a prova da infração não pode ser realizada por outros meios. Esses são requisitos, como se viu, para a interceptação (telefônica, telegráfica ou telemática), medida de natureza diversa e disciplinada pela Lei n. 9.296/96. A quebra do sigilo informacional (sigilo de dados), assim entendida a requisição mediante ordem judicial de registros de conexão e acesso a aplicações de Internet, de forma autônoma ou associados a outros dados pessoais e informações, não exige que a autoridade expedidora da ordem indique previamente as pessoas que estão sendo investigadas, até porque o objetivo dessa medida, na maioria dos casos, é justamente de proporcionar a identificação do usuário do serviço ou do terminal utilizado.

É a própria Lei que estabelece os requisitos para que a medida de requisição de registros de

tráfego na Internet e dados pessoais armazenados em poder do provedor possa ser considerada proporcional e razoável. Se a autoridade judicial, ao fundamentar a quebra do sigilo de dados, preenche os requisitos traçados nos incisos I a III do art. 22 da Lei 12.965/14, a medida não pode ser considerada abusiva ou desproporcional. A Lei específica, que disciplina a requisição para acesso a registros de tráfego na Internet e dados pessoais coletados por provedores, não faz exigência que a ordem judicial indique os suspeitos da prática delituosa investigada ou a demonstração de inexistência de outros meios de prova, menos restritivos e mais eficazes. Esses não são requisitos legais ou que decorram de algum princípio constitucional.

É incompatível com a natureza da medida de requisição de registros e dados, com fins de investigação de ilícitos, que se indique previamente os autores da infração ou crime objeto da investigação. Como vai se exigir que a autoridade requisitante indique os nomes de pessoas que passaram por um determinado local, em determinado espaço de tempo, se é justamente isso que ela pretende descobrir por meio da requisição enviada ao provedor?

O que é razoável exigir, nesse tipo de investigação, é que a autoridade requisitante justifique a medida através da indicação de motivos que façam crer a existência do crime investigado (tal como previsto no inc. I do art. 22 da Lei 22 da Lei 12.965/14). Isso é o que vem sendo feito. A Justiça tem deferido pedidos de acesso a dados de localização de telefones celulares em determinadas áreas geográficas. Antes de requerer o fornecimento de dados de geolocalização a provedores de aplicações na Internet, as ordens eram destinadas às operadoras de telefonia, que conseguem fornecer esses dados por meio da

triangulação de células (antenas) da rede de telefonia móvel. As operadoras de telefonia móvel são capazes de saber, por exemplo, os números de telefones celulares de pessoas que transitaram por determinada área em específico período de tempo, por meio das coordenadas de latitude e longitude das torres (antenas) próximas. O processo de localização por triangulação de células permite revelar o local em que um usuário da rede de telefonia móvel estava em determinado momento. Os dados de localização aparecem em razão dos registros que apontam em qual antena (torre de celular) o equipamento estava conectado em determinado momento. Esses dados de geolocalização já vêm sendo usados como precioso recurso na investigação de crimes. Além dos dados de conexão a torres de celular, dados de GPS também vêm sendo usado há anos nos tribunais. Por meio da triangulação por tempo real, a operadora pode apontar o local exato de um aparelho, e ainda acompanhá-lo à medida em que se move²⁸.

Portanto, a ordem judicial para quebra do sigilo de dados, delimitada por coordenadas geográficas (como local da execução do crime ou áreas onde transitaram os agentes criminosos) em certo lapso de tempo, nada tem de desproporcional ou extrema. Muito pelo contrário. A

²⁸ Em relação aos **dados telefônicos**, não depende de prévia autorização judicial o acesso pela autoridade policial à agenda eletrônica e aos registros de ligações (histórico de chamadas) (STF, HC 91.867, Rel. Min. Gilmar Mendes, 19/09/2012; STJ, HC 66.368, Rel. Min. Gilson Dipp, DP 29/06/2007). Da mesma forma, o delegado de polícia pode requisitar, junto à operadora de telefonia, acesso aos dados de localização pretéritos, que são os registros de conexão às ERB's (Estações Rádio Base) às quais o investigado conectou o celular (STJ, HC 247.331, Rel. Min. Maria Thereza de Assis Moura, DJe 03/09/2014). Todos esses dados são estáticos e não revelam o conteúdo da comunicação. Todavia, para a obtenção de dados de localização em tempo real, o entendimento é pela necessidade da prévia chancela judicial. O legislador abriu uma exceção parcial para os casos de investigação de crime de tráfico de pessoas (artigo 149-A do CP), cuja autorização judicial pode ser dispensada se não houver manifestação judicial no prazo de 12 horas, em verdadeira *cláusula de reserva de jurisdição temporária* (art. 13-B, § 4º., do CPP, na redação dada pela Lei n. 13.344/16).

delimitação já funciona como fator que estreita a quebra do sigilo informacional, reduzindo a medida para o limite necessário à descoberta da autoria ou outros aspectos do crime investigado. O importante é que não seja excessiva ou mais invasiva do que o necessário para possibilitar a investigação do delito ou fato ilícito. A indicação na decisão de um limite geográfico e de um lapso temporal, para a recolha das informações, são elementos que servem como parâmetros indicativos da proporcionalidade da medida de quebra do sigilo informacional.

Ainda que a quebra do sigilo de dados não resulte em um sucesso completo para a investigação ou não forneça todos os elementos para a elucidação do crime, isso em nada afeta a legalidade da medida. É suficiente que os dados requisitados possam servir de alguma maneira como meio de prova, que tenham algum potencial de utilidade para a investigação (tal como previsto no inc. II do art. 22 da Lei 22 da Lei 12.965/14). O que justifica a ordem para quebra do sigilo informacional não é a garantia de que os autores serão identificados e o crime solucionado, mas a necessidade de investigá-lo.

Além disso, os registros de acesso e utilização de aplicações na Internet (e outros dados pessoais a eles vinculados) não necessitam ter uma acuidade ou precisão absolutas. Se existem estudos técnicos que indicam que especialmente os dados de geolocalização podem ser imprecisos, cabe ao Juiz avaliar o grau de falibilidade desses dados, no momento de decidir pela sua utilização como meio de prova no processo. Ainda que não suficientemente precisos, os dados fornecidos pelo provedor de Internet podem servir para identificar o autor da infração ou apenas como mais um elemento de prova que,

corroborado por outros elementos de convicção carreados aos autos, sirva para a investigação ou instrução probatória.

6- A ordem judicial de quebra de sigilo baseada em coordenadas geográficas (e/ou períodos de tempo) em regra envolve "dados anonimizados", que não permitem identificar a pessoa a quem se referem

A possibilidade de a quebra de sigilo informacional baseada em coordenadas geográficas e períodos temporais definidos, entregar informações de outras pessoas que não tenham nenhuma relação com o fato ilícito investigado também não atribui à medida caráter desproporcional ou exagerado. A requisição tem uma única finalidade que é a utilização das informações recebidas para fins de investigação do ilícito ou instrução probatória. Os dados recebidos não podem ser utilizados para outra finalidade. Qualquer informação recebida que não tenha relação com o objetivo da ordem judicial deve ser protegida (ou descartada) e não utilizada para outra finalidade, nem muito menos revelada a terceiros. Os dados de pessoas não envolvidas com o fato objeto da ordem judicial continuam protegidos pelo sigilo informacional, cuja violação inclusive é tipificada criminalmente.

Além disso, em regra os dados de geolocalização que são fornecidos em atendimento a ordens judiciais de quebra de sigilo baseadas em coordenadas geográficas não permitem identificar de logo as pessoas a que se referem. São dados anonimizados, que não proporcionam a identificação dos titulares²⁹. No caso que

²⁹ O inc. III do art. 5º. da nova LGPD (Lei n. 13.709/18) conceitua **dado anonimizado** como o "dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e

decidi, por exemplo, foram solicitados apenas os números identificadores (N-ID)³⁰ de aparelhos celulares que transitaram na área da cena do crime, dentro de determinado período de tempo (das 5:00 às 8:00h do dia 06.05.18, data do crime de homicídio), acompanhados dos registros de localização. O próprio Juiz que expediu a ordem de quebra do sigilo informacional, Dr. André Simões Nunes, explicou que, com essa medida, os usuários de serviços da Google não teriam suas identidades reveladas e, somente depois, quando a autoridade policial fizesse uma análise daqueles números (números ID) que aparecessem com maior frequência na área da cena do crime, é que a investigação seria estreitada para eles e, em seguida, solicitada nova ordem judicial, desta feita para identificação dos titulares dos aparelhos. Confira-se o trecho da decisão judicial, onde o magistrado deixou bem aclarado esse ponto, mostrando que a ordem de quebra do sigilo informacional é insuscetível de produzir efeitos colaterais sobre a privacidade de terceiros não envolvidos com o delito, pela simples razão de que os dados solicitados não permitiam identificar as pessoas:

“Aqui, em complementação ao que já foi dito acima, é preciso salientar que a presente representação não objetiva ter acesso irrestrito aos dados dos usuários presentes nas localidades indicadas na peça processual. **Tais usuários sequer terão suas identidades reveladas.** Pelo contrário, serão fornecidos apenas os números

disponíveis na ocasião de seu tratamento”. Aqui estamos utilizando *dado anonimizado* com um conceito mais largo, de não somente o dado que, originariamente relativo a uma pessoa, passa por técnicas que garantem sua desvinculação a ela. O conceito é utilizado aqui como todo e qualquer dado que não permite identificar a pessoa do titular.

³⁰Cada *smartphone* com sistema *Android* tem um número próprio de registro ID.

identificadores (N-ID) dos celulares presentes no raio de 200 (duzentos) metros de cada ponto de referência, sem qualquer menção à qualificação dos titulares de referidos aparelhos.

Após, será realizada a análise comparativa dos registros das diversas localidades, de modo a se identificar aqueles números identificadores (N-ID) que constem de mais de um setor, hipótese em que deverá ser solicitada nova deliberação judicial, esta sim com a finalidade de possibilitar o conhecimento dos titulares dos respectivos aparelhos celulares".
(grifamos)

Como se vê, o efeito colateral de medida de quebra de sigilo de dados baseada em coordenadas geográficas pode ser nenhum. A requisição em geral envolve dados que não identificam os titulares, sem qualquer risco de invasão desproporcional na privacidade alheia. A requisição, como ocorreu no caso mencionado, permitiu identificar os aparelhos que transitaram nas imediações da área delimitada como a "cena do crime", mas não os proprietários dos aparelhos. Provavelmente, somente os aparelhos que aparecessem (por meio dos dados de geolocalização) concomitantemente no local da execução do crime e nas rotas de perseguição da vítima e de fuga dos executores é que seriam selecionados para investigação mais aprofundada e aí, certamente, a autoridade policial iria solicitar nova ordem judicial para ter acesso a outros dados que permitam identificar os usuários desses aparelhos.

Se nessa segunda fase da investigação, a autoridade policial necessitar apenas de dados cadastrais dos usuários de determinados aparelhos, aí nem sequer será necessário tomar iniciativa através do Poder Judiciário para fazer a requisição à Google, isso porque não há necessidade de se obter um mandado judicial para se requisitar esse tipo de dados.

A Lei n. 12.965/14 é ainda mais flexível no que tange à requisição de dados cadastrais dos usuários de serviços e aplicações na Internet. Por intermédio das informações cadastrais pode ser obtido o nome do cliente, RG, CPF, endereço completo, telefones para contato e endereço de e-mail, por exemplo³¹. O levantamento dessas informações, para fins de instruir processo penal ou cível, não necessita sequer de ordem judicial, sendo suficiente uma mera solicitação de autoridade administrativa. Nos termos do § 3º. do art. 10 da Lei, o acesso aos dados cadastrais que informem qualificação pessoal, filiação e endereço pode ser realizado “pelas **autoridades administrativas** que detenham competência legal para a sua requisição”. O Decreto n. 8.771, de 11 de maio de 2016 (que regulamentou a Lei n. 12.965/14), não especificou quem são as “autoridades administrativas” autorizadas a ter acesso aos dados cadastrais de usuários em poder dos provedores, mas é óbvio que a autoridades policiais e integrantes do Ministério Público estão compreendidos nesse conceito³².

³¹ Nos termos do § 2º. do art. 11 do Decreto n. 8.771/16, “são considerados **dados cadastrais**: I - a filiação; II - o endereço; e III - a qualificação pessoal, entendida como nome, prenome, estado civil e profissão do usuário.”

³² O art. 13-A do Código de Processo Penal (incluído pela Lei n. 13.344/16) prevê que, para fins de investigação de certos crimes graves (como, p. ex., sequestro, cárcere privado, tráfico de órgãos e de pessoas, trabalho escravo, adoção ilegal, exploração sexual e extorsão), o membro do Ministério Público ou o delegado de polícia poderá requisitar diretamente “de quaisquer órgãos do poder público ou de empresas da iniciativa privada, **dados e informações cadastrais** da vítima ou de suspeitos”. O artigo 15 da Lei 12.850/13 (que define

Para possibilitar o prosseguimento das investigações, quando já tiver definido quais aparelhos celulares transitaram pelos locais da “cena do crime” com mais intensidade, a autoridade policial necessitará especificar tão somente que o provedor informe os dados cadastrais dos usuários desses aparelhos³³.

7- Posição da jurisprudência brasileira - acórdão do TJSE

A Justiça brasileira vem se inclinando a conceder quebra de sigilo de dados com base em coordenadas geográficas e delimitadas por espaço temporal.

Recentemente, o Pleno do Tribunal de Justiça de Sergipe, por expressiva maioria de votos, manteve decisão que obrigou a Google Brasil a fornecer dados de um grupo não identificado de pessoas que passaram por um local em que houve um homicídio. O caso envolveu a apuração do assassinato de um capitão da Polícia Militar daquele Estado, ocorrido em 04 de abril de 2018, no município de Porto da Folha (SE). Durante a investigação, foi solicitada pela autoridade policial a quebra do sigilo de dados. O Juiz da Comarca de Porto da Folha autorizou a medida, determinando que a Google fornecesse informações de conexão e de acesso a aplicações de Internet e outros dados (contas, nomes de usuário, e-mail, números de IP e de Imei) das pessoas que estariam próximas ou no local do crime e utilizando os serviços da empresa durante o horário estimado do crime (entre 22:40 e 22:55h).

“organização criminosa”) e o artigo 17-B da Lei 9.613/98 (que dispõe sobre os crimes de “lavagem” ou ocultação de bens, direitos e valores) também admitem que a Polícia Judiciária e o Ministério Público possam ter acesso a dados cadastrais de investigados, independentemente de ordem judicial.

³³ Nos termos do parágrafo 3º. do art. 11 do Decreto n. 8.771/16.

A Google impetrou mandado de segurança no TJSE³⁴ com a mesma fundamentação do presente *mandamus*, ou seja, de que a ordem era ilegal e inconstitucional, pois determinara a quebra de sigilo de um conjunto não identificado de pessoas, sem individualizá-las, apenas por terem transitado por certas coordenadas geográficas, em certo período de tempo. Segundo a empresa, a legislação vigente veda pedidos genéricos de quebra de sigilo de dados telefônicos e telemáticos, sendo imprescindível a individualização das pessoas que serão afetadas pela medida. Apontou, ainda, que a medida era desproporcional, inadequada e desnecessária, pois poderia atingir a privacidade de pessoas inocentes sem garantias de se chegar aos autores do crime investigado, em violação aos incisos X e XII do artigo 5º da Constituição Federal.

O TJSE negou o pedido da Google, pois entendeu que a decisão do Juiz da Comarca de Porto da Folha encontra respaldo no artigo 22 do Marco Civil da Internet e se limitou às informações de conexão e de acesso a aplicações de internet, não abrangendo o conteúdo das comunicações. Segundo a relatora, Desembargadora Iolanda Santos Guimarães, o sistema jurídico brasileiro tutela de maneira diferente a proteção ao conteúdo das comunicações mantidas entre indivíduos e a conferida às informações de conexão e de acesso a aplicações de internet, garantindo uma menor proteção a essa segunda categoria de dados. A relatora afirmou ainda que para a quebra do sigilo de dados em poder de provedor de Internet é suficiente que sejam preenchidos os requisitos do art. 22 do Marco Civil da Internet, ou seja, que a autoridade requisitante indique a existência de um ilícito (inc. I), a necessidade da medida

³⁴ Mandado de Segurança Cível n. 201800111901, relatora Desembargadora IOLANDA SANTOS GUIMARÃES, j. 22.08.18.

para a investigação (inc. II) e o período de tempo ao qual se referem os dados (inc. III)³⁵.

A ementa desse julgado ficou assim redigida:

“Constitucional e Processo Penal - Mandado de Segurança - Inquérito policial - Investigação do homicídio do Comandante da Companhia Independente de Operações Policiais Especiais em área de Caatinga (CIOPAC) - **Decisão que determina a quebra de sigilo telemático** - Pleito de anulação - **Invocação da proteção da privacidade e do sigilo das comunicações prevista no art. 5º, incisos X e XII, da Constituição Federal - Leis n os 9.296/96 (interceptação de comunicações telefônicas) e 12.965/2014 (Marco Civil da Internet) que regulamentam os dispositivos constitucionais - Diferença na tutela dada pela legislação ao conteúdo das comunicações mantidas entre indivíduos e às informações de conexão e de acesso a aplicações de internet - Menor proteção do sistema jurídico às informações de conexão e de acesso a aplicações de internet - Requerimento da Autoridade Policial limitado às informações de conexão e de acesso a aplicações de internet (contas, nomes de usuário, números de IP que foram usados associados a smartphones com sistema Android, número de IMEI e e-mail associados**

³⁵ Ver notícia sobre esse julgamento publicada no site Conjur, no dia 04.07.19, sob o título: “TJ de Sergipe autoriza quebra genérica de sigilo de dados baseada na localização”, acessível em: <https://www.conjur.com.br/2019-jul-04/tj-permite-quebra-generica-sigilo-dados-baseada-localizacao>

aos aparelhos e usuários que recorreram aos serviços dos Impetrantes) em um determinado período de tempo e numa área delimitada - Inexistência de pedido de quebra do sigilo do conteúdo de comunicações eventualmente transmitidas pelas pessoas a serem atingidas pela medida excepcional - Observância do disposto no art. 22 do Marco Civil da Internet - Existência de ilícito criminal (art. 22, inciso I, do Marco Civil), necessidade da medida para o prosseguimento das investigações (art. 22, inciso II, do Marco Civil) e limitação das áreas e dos períodos de tempo dos registros (art. 22, inciso III, do Marco Civil) - Registros limitados a um período de 15 (quinze) minutos, em horário noturno, em rodovia estadual pouco movimentada - Segurança denegada.

I - Cuida-se de mandado de segurança que objetiva anular a **decisão proferida pelo Juízo Impetrado que, acolhendo requerimento da Autoridade Policial, quebrou o sigilo telemático de pessoas não identificadas**, medida adotada nos autos do Inquérito Policial que investiga o homicídio que vitimou o Capitão da Polícia Militar do Estado de Sergipe Manoel Alves de Oliveira Santos, então Comandante da Companhia Independente de Operações Policiais Especiais em área de Caatinga (CIOPAC), no dia 04/04/2018, por volta das 20h, na

Rodovia Estadual SE200, no Município de Porto da Folha/SE;

II - A Constituição Federal protege, nos incisos X e XII do seu art. 5º, a privacidade e o sigilo das comunicações, garantias essas regulamentadas pela Lei nº 9.296/96 (interceptação de comunicações telefônicas) e pela Lei nº 12.965/2014 (Marco Civil da Internet);

III - A leitura dos citados diplomas legais revela que o sistema jurídico diferencia a tutela dada ao conteúdo das comunicações mantidas entre indivíduos e às informações de conexão e de acesso a aplicações de internet, garantindo uma maior proteção ao primeiro e flexibilizando a proteção da segunda;

IV - No caso dos autos, a medida combatida se limitou a atender requerimento que, por sua vez, restringiu-se à quebra do sigilo das informações de conexão e de acesso a aplicações de internet (contas, nomes de usuário, números de IP que foram usados associados a smartphones com sistema Android, número de IMEI e email associados aos aparelhos e usuários que recorreram aos serviços dos Impetrantes) em um determinado período de tempo e numa área delimitada, tudo isso no bojo de investigação de um homicídio;

V - Não houve qualquer requerimento por parte da Autoridade Policial quanto à quebra do sigilo do conteúdo das

comunicações eventualmente transmitidas pelas pessoas a serem atingidas pela medida excepcional;

VI - **Nesse quadro, os requisitos do art. 22 do Marco Civil da Internet para a manutenção da medida se mostram presentes: há um ilícito, inclusive de natureza criminal (inciso I); a Autoridade Policial explicitou ser imprescindível a medida para a continuidade das investigações, com a identificação dos suspeitos (inciso II); e o requerimento foi delimitado não só no tempo, mas na área a ser atingida (inciso III);**

VII - Vale destacar, das informações prestadas pelo Juízo Impetrado, que o lapso temporal é entre "(...) 04 de abril de 2018 às 22h40min e 04 de abril de 2018 às 22h55m, ou seja, são apenas 15 minutos" de dados em "(...) local ermo, estrada de difícil acesso, de restrita circulação de pessoas, especialmente no horário indicado (...)", indicando que um número mínimo de pessoas eventualmente será atingida pela quebra do sigilo;

VIII - Segurança denegada."³⁶

A Google ainda tentou suspender a ordem por meio de recurso aviado ao Superior Tribunal de Justiça³⁷, mas o Ministro Nefi Cordeiro negou o pedido de liminar por

³⁶ O teor integral do acórdão pode ser acessado em: <https://www.conjur.com.br/dl/tj-quebra-sigilo-generica-baseada-tempo.pdf>

³⁷ RMS n. 61215, Sexta Turma, rel. Min. Nefi Cordeiro.

entender se tratar de recurso em mandado de segurança, cabível apenas em situações de flagrante constrangimento ilegal – situação não verificada nos autos, segundo ele. O mérito ainda será analisado³⁸.

Como se observa, existe respaldo na legislação brasileira para requisição de dados pessoais armazenados por provedor de aplicações de Internet, com delimitação apenas por coordenadas geográficas ou período de tempo, sem necessidade portanto de individualização das pessoas suspeitas de cometer a infração objeto da investigação. A jurisprudência convalida ordem de tal natureza, conforme se denota do mencionado acórdão do TJSE³⁹.

8- Dados coletados pelos provedores devem ser mantidos "em formato interoperável e estruturado, para facilitar o acesso decorrente de decisão judicial ou determinação legal" (art. 15 do Decreto n. 8.771/16)

Todo e qualquer tipo de dado coletado por provedores de serviços na Internet (por meio de sites, plataformas e aplicativos) podem ser utilizados para fins de investigação policial ou instrução processual (em

³⁸ Ver notícia publicada no site do STJ em 04.07.19, sob o título: "Google não consegue suspender quebra de sigilo de dados de grupo de usuários não identificados", acessível em: <http://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/Google-nao-consegue-suspender-quebra-de-sigilo-de-dados-de-grupo-de-usuarios-nao-identificados.aspx>

³⁹ Note-se inclusive que a quebra do sigilo de dados no caso citado foi bem mais ampla que a determinada pelo Juiz da Comarca de Jupi-PE. Naquele outro caso julgado pelo TJSE, a requisição judicial envolveu dados como contas, nomes de usuário, números de IP que foram usados associados a *smartphones* com sistema *Android*, números de IMEI e endereços de *email* associados aos aparelhos e usuários que recorreram aos serviços do provedor. Na decisão do Juiz de Jupi, apenas foram requisitados os números identificadores (N-ID) dos celulares, associados aos dados de localização dos aparelhos.

processo cível ou penal), respeitadas as prescrições legais. Não somente registros de conexão (*logs*) à rede e aplicações, mas todos os dados de natureza pessoal ou não (como dados anonimizados e metadados), que decorram de qualquer operação de coleta, guarda ou tratamento realizada por provedores de conexão e aplicações de Internet podem ser requisitados pelas autoridades judiciais para possibilitar a investigação de ilícitos e facilitar a atividade de persecução penal. **Os provedores inclusive têm a obrigação de manter os dados armazenados em seus servidores "em formato interoperável e estruturado, para facilitar o acesso decorrente de decisão judicial ou determinação legal"** (art. 15 do Decreto n. 8.771/16).

9- Provedor não pode dar ciência a seus usuários sobre ordem que recebe para entrega de dados, sob pena de ser responsabilizado

Além de se notabilizar pela resistência frequente ao cumprimento de requisições judiciais para a entrega de dados, a Google também vem se utilizando de outro expediente para tentar minar as ordens de quebra de sigilo informacional. Tem comunicado aos seus usuários sempre que recebe ordens para a entrega de dados sob sua guarda, ainda quando os dados requisitados não tenham natureza de dado pessoal ou possam de alguma maneira identificar o usuário. Trata-se de expediente para instigar os usuários a contestarem judicialmente as ordens judiciais que ela própria tem interesse em confrontar, pois nas comunicações que vem fazendo chega a dar prazo para que o usuário consiga uma contraordem antes que realize a entrega

do material informacional⁴⁰. Como a Google não tem tido muito sucesso nos tribunais em contestar, *sponte sua*, as requisições judiciais para entrega de dados (até porque não tem *legitimidade* para fazer a defesa da privacidade dos titulares), então vem instigando os usuários a tomar a iniciativa que em última análise só interessa a ela própria, pois na maioria dos casos as requisições judiciais envolvem dados que não são capazes de identificar o usuário ou de qualquer maneira invadir sua privacidade.

Esse tipo de conduta é ilegal e pode ensejar a adoção de penalidades, como imposição de multas⁴¹ e até sanções mais pesadas, pois constitui forma de minar a eficácia da ordem judicial e pode ter o efeito de prejudicar a investigação em andamento.

Diga-se que a Google é conhecida não apenas por tentar minar a eficácia de requisições para entrega de dados, mas também ordens judiciais de outra natureza. Isso vem ocorrendo em relação aos requerimentos de *desindexação* nos motores de busca na Internet, que são feitos por pessoas interessadas em não ter seus nomes aparecendo em resultados de pesquisa em relação a fatos que não tenham

⁴⁰ Pelo menos é o que se depreende que a Google vem fazendo ao se ler reportagem publicada pelo site da NBC, em 07.03.20, que relata o caso envolvendo Zachary McCoy, um cidadão residente na cidade de Gainesville, Flórida (nos EUA), que achou que se tornou suspeito de um assalto em uma casa nas cercanias do seu trajeto corriqueiro de bicicleta, apenas por ter recebido uma comunicação da Google de que entregaria seus dados à polícia local para investigação do crime. Sem a Google ter explicado exatamente quais dados seriam entregues - a comunicação mencionou apenas dados vinculados à conta do usuário - e assustado com a possibilidade de ser considerado suspeito de um crime que não cometera, McCoy contratou advogado e prematuramente contestou a ordem. A notícia sobre esse caso está acessível em: <https://www.nbcnews.com/news/us-news/google-tracked-his-bike-ride-past-burglarized-home-made-him-n1151761>

⁴¹ O Juiz de Direito da Comarca de Jupi-PE, ao requisitar os dados de localização para identificar os executores de um crime de homicídio, na mesma decisão aplicou multa para a hipótese de a Google comunicar seus usuários, no valor de dez mil reais por cada notificação que viesse a fazer, "sem prejuízo das demais medidas legais cabíveis" (Proc. n. 000221-43.2019.8.17.0850).

relevância social ou interesse público⁴². Ao invés de se limitar a retirar dos resultados das pesquisas os *links* contendo as notícias, quando atende a um requerimento ou recebe notificação judicial, a Google tem dado ciência aos controladores dos *sites* onde o conteúdo ilícito está hospedado, permitindo que eles tornem pública a desindexação ou simplesmente transfiram o material para outra página no próprio site ou em outro endereço na *web*. Por conta desse tipo de prática, a Google já recebeu multa de autoridades de proteção de dados em vários países⁴³.

10- Conclusões:

1ª.) Embora o provedor figure como destinatário da ordem judicial, para se contrapor a uma requisição para entrega de dados tem que apontar algum interesse ou direito de sua titularidade que possa ser atingido pela quebra do sigilo telemático. O que não pode é contestar a ordem judicial pretendendo a defesa da privacidade de terceiros, por não ser *representante* deles e nem lhe ser conferida pela lei a qualidade de *substituto processual*. Qualquer pessoa que se

⁴² Para quem quiser se informar melhor sobre o "direito à desindexação", sugerimos a leitura de nosso artigo intitulado "A remoção dos resultados de pesquisa (indexação) dos motores de busca na internet (1ª parte). A repercussão da decisão do Tribunal de Justiça da União Europeia". **Revista Jus Navigandi**, ISSN 1518-4862, Teresina, ano 19, n. 4039, 23 jul. 2014. Disponível em: <https://jus.com.br/artigos/30429> .

⁴³ Recentemente, a Google recebeu uma pesada multa da autoridade de proteção de dados da Suécia - ver notícia publicada no site *Tecmundo*, em 12.03.20, acessível em: <https://www.tecmundo.com.br/internet/151034-google-multada-r-37-milhoes-suecia.htm>. Antes disso, já havia sido multada pela autoridade de proteção de dados da Espanha, mas conseguiu reverter a multa na Justiça espanhola, que entendeu que como o "direito à desindexação" era de construção jurisprudencial e não tinha contornos bem definidos, ainda não se sabendo se o motor de busca tinha o direito de comunicar os controladores de sites sobre a medida adotada, não era razoável punir a Google antes desse aspecto ficar bem definido - ver matéria publicada em 27.05.19, acessível em: https://www.eldiario.es/tecnologia/Audiencia-Nacional-Proteccion-Datos-Google_0_903610208.html

sentir lesada, por entender que a ordem alcança sua órbita de interesses, pode individualmente fazer a defesa de eventuais direitos lesados.

2ª.) Os provedores de serviços na Internet não são os titulares e não podem pretender um monopólio sobre os dados que coletam e armazenam. Exigências de ordem social e razões fundadas no interesse público podem justificar a entrega dos dados pessoais coletados pelos sistemas informatizados de empresas privadas às autoridades públicas. A necessidade de viabilizar uma investigação criminal ou a instrução de um processo judicial é um exemplo de situação excepcional que pode autorizar a quebra do sigilo informacional.

3ª.) Leis diferentes (Lei n. 9.296/96 e Lei n. 12.965/14) disciplinam com requisitos diversos o procedimento da requisição judicial para entrega de dados armazenados pelo provedor e o da interceptação das comunicações (telefônica, telegráfica ou telemática). O art. 22 da Lei 12.965/14 ("Marco Civil da Internet") não exige que a ordem para quebra do sigilo informacional (sigilo de dados) tenha que, obrigatoriamente, indicar os "alvos" da investigação ou que o magistrado precise de alguma maneira qualificar previamente na sua decisão as pessoas suspeitas de cometer o ilícito investigado.

4ª.) O propósito primário da quebra do sigilo informacional é justamente a descoberta da autoria de crimes, através do levantamento de registros, dados pessoais e "**outras informações que possam contribuir para a identificação do usuário**" de um serviço na Internet ou terminal conectado à rede (parágrafo 1º. do art. 10 da Lei 12.965/14), daí ser

incompatível com a natureza e objetivos dessa medida a exigência de descrição ou qualificação prévia de qualquer pessoa a quem os dados requisitados se referem. É ilógico se exigir que a autoridade expedidora da ordem descreva a(s) pessoa(s) alvo(s) da quebra do sigilo informacional quando a finalidade dessa medida é justamente proporcionar a descoberta da identidade de quem fez uso do serviço ou acessou um determinado terminal, em algum momento e em certa localidade.

5ª.) As restrições formais e procedimentais elencadas na Lei n. 9.296/96 (e na Resolução CNJ n. 59/2008) não são aplicáveis por extensão ou analogia à quebra de sigilo de dados, sobretudo quando a ordem é dirigida a um provedor de serviço de conexão ou aplicações de Internet. Isso porque a lei específica que disciplina a requisição judicial de dados pessoais em poder dos provedores, para fins de investigação de ilícitos ou instrução processual (Lei n. 12.965/14), não elenca, dentre os requisitos que estabelece para a quebra do sigilo informacional, que a ordem judicial especifique previamente as pessoas objeto da investigação ou que a prova da infração (ou da autoria) possa ser realizada por outros meios.

6ª.) Para o Juiz requisitar dados pessoais armazenados por provedor de serviços de Internet, basta fundamentar sua decisão com os seguintes elementos: a) indícios da ocorrência do ilícito; b) justificativa da utilidade da requisição; e c) período ao qual se referem os registros (incisos I a III do art. 22 da Lei 12.965/14). Se a autoridade judicial, ao fundamentar a quebra do sigilo de dados, preenche esses requisitos, a medida não pode ser considerada abusiva ou desproporcional.

7ª.) A ordem judicial para quebra do sigilo de dados, delimitada por coordenadas geográficas (como local da execução do crime ou áreas onde transitaram os agentes criminosos) em certo lapso de tempo, nada tem de desproporcional ou extrema. Muito pelo contrário. A delimitação já funciona como fator que estreita a quebra do sigilo informacional, reduzindo a medida para o limite necessário à descoberta da autoria ou outros aspectos do crime investigado. A indicação na decisão de um limite geográfico e de um lapso temporal, para a recolha das informações, são elementos que servem como parâmetros indicativos da proporcionalidade da medida de quebra do sigilo informacional.

8ª.) Ainda que a quebra do sigilo de dados não resulte em um sucesso completo para a investigação ou não forneça todos os elementos para a elucidação do crime, isso em nada afeta a legalidade da medida. É suficiente que os dados requisitados possam servir de alguma maneira como meio de prova, que tenham algum potencial de utilidade para a investigação (tal como previsto no inc. II do art. 22 da Lei 22 da Lei 12.965/14). O que justifica a ordem para quebra do sigilo informacional não é a garantia de que os autores serão identificados e o crime solucionado, mas a necessidade de investigá-lo.

9ª.) Os registros de acesso e utilização de aplicações na Internet (e outros dados pessoais a eles vinculados) não necessitam ter uma acuidade ou precisão absolutas. Cabe ao Juiz avaliar o grau de falibilidade desses dados, no momento de decidir pela sua utilização como meio de prova no processo. Ainda que não suficientemente precisos, os

dados fornecidos pelo provedor de Internet podem servir para identificar o autor da infração ou apenas como mais um elemento de prova que, corroborado por outros componentes de convicção carreados aos autos, sirva para a investigação ou instrução probatória.

10^a.) A possibilidade de a quebra de sigilo informacional baseada em coordenadas geográficas e períodos temporais definidos, entregar informações de outras pessoas que não tenham nenhuma relação com o fato ilícito investigado também não atribui à medida caráter desproporcional ou exagerado. A requisição tem uma única finalidade que é a utilização das informações recebidas para fins de investigação do ilícito ou instrução probatória. Os dados recebidos não podem ser utilizados para outra finalidade. Qualquer informação recebida que não tenha relação com o objetivo da ordem judicial deve ser protegida (ou descartada) e não utilizada para outra finalidade, nem muito menos revelada a terceiros. Os dados de pessoas não envolvidas com o fato objeto da ordem judicial continuam protegidos pelo sigilo informacional, cuja violação inclusive é tipificada criminalmente.

11^a.) A ordem judicial de quebra de sigilo baseada em coordenadas geográficas (e/ou períodos de tempo) em regra envolve "dados anonimizados", que não permitem identificar a pessoa a quem se referem. Assim, o efeito colateral de medida de quebra de sigilo de dados baseada em coordenadas geográficas pode ser nenhum. A requisição em geral envolve dados que não identificam os titulares, sem qualquer risco de invasão desproporcional na privacidade alheia.

12ª.) A Lei n. 12.965/14 é ainda mais flexível no que tange à requisição de dados cadastrais dos usuários de serviços e aplicações na Internet. O levantamento dessas informações, para fins de instruir processo penal ou cível, não necessita sequer de ordem judicial, sendo suficiente uma mera solicitação de autoridade administrativa (§ 3º. do art. 10 da Lei n. 12.965/14)

13ª.) Todo e qualquer tipo de dado coletado por provedores de serviços na Internet (por meio de sites, plataformas e aplicativos) podem ser utilizados para fins de investigação policial ou instrução processual (em processo cível ou penal), respeitadas as prescrições legais. Não somente registros de conexão (*logs*) à rede e aplicações, mas todos os dados de natureza pessoal ou não (como dados anonimizados e metadados), que decorram de qualquer operação de coleta, guarda ou tratamento realizada por provedores de conexão e aplicações de Internet podem ser requisitados pelas autoridades judiciais para possibilitar a investigação de ilícitos e facilitar a atividade de persecução penal. **Os provedores inclusive têm a obrigação de manter os dados armazenados em seus servidores "em formato interoperável e estruturado, para facilitar o acesso decorrente de decisão judicial ou determinação legal"** (art. 15 do Decreto n. 8.771/16).

14ª.) Provedor não pode dar ciência a seus usuários sobre ordem que recebe para entrega de dados, sob pena de ser responsabilizado. Esse tipo de conduta é ilegal e pode ensejar a adoção de penalidades, como imposição de multas e até sanções mais pesadas, pois constitui forma de minar a eficácia da ordem judicial e pode ter o efeito de prejudicar a investigação em andamento.