TRIBUNAL DE JUSTIÇA DO ESTADO DE SERGIPE

ACÓRDÃO:	201818567
RECURSO:	Mandado de Segurança Cível
PROCESSO:	201800111901
RELATOR:	IOLANDA SANTOS GUIMARÃES

IMPETRANTE	GOOGLE BRASIL INTERNET LTDA	Advogado: EDUARDO BASTOS FURTADO DE MENDONÇA
IMPETRANTE	GOOGLE LLC	Advogado: EDUARDO BASTOS FURTADO DE MENDONÇA
IMPETRADO	JUIZO DE DIREITO DA COMARCA DE PORTO DA FOLHA	

EMENTA

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 nºs 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 limitada 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 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 SE-200, 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 e-mail 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.

ACÓRDÃO

Vistos, relatados e discutidos os presentes autos, acordam os integrantes do Tribunal de Justiça do Estado de Sergipe, em sua composição plenária, por maioria, conhecer do *writ* para denegar a segurança pleiteada, em conformidade

com o relatório e voto constantes dos autos, que ficam fazendo parte integrante do presente julgado.

Aracaju/SE, 22 de Agosto de 2018.

DESA. IOLANDA SANTOS GUIMARÃES
RELATOR

RELATÓRIO

Desembargadora Iolanda Santos Guimarães (Relatora): – Trata-se de Mandado de Segurança impetrado pelo *Google Brasil Internet Ltda.* e *Google LLC.* contra ato do *Juízo de Direito da Comarca de Porto da Filha*, o qual teria proferido decisão autorizando a quebra do sigilo telemático de um conjunto de pessoas não identificadas nos autos de Inquérito Policial.

Em síntese, os Impetrantes sustentam, inicialmente, o cabimento do *mandamus* com base no disposto no art. 5º, inciso II, da Lei nº 12.016/2009 (Lei do Mandado de Segurança), que prevê ser cabível a sua impetração para impugnar decisões judiciais irrecorríveis.

Prosseguindo, defendem ser inconstitucional e ilegal a medida determinado pela Autoridade Impetrada, invocando o teor do art. 5º, incisos X e XII, da Constituição Federal, que protegem o direito à privacidade e das comunicações, destacando, ainda, o disposto no art. 93, inciso IX, da CF/88 para apontar a ausência de fundamentação específica na decisão questionada.

Aduz, a esse respeito, que "(...) a quebra do sigilo é medida excepcional e, por isso mesmo, só poderia ser justificada pela existência de indícios concretos de atividade ilícita por parte do alvo, a serem demonstrados em decisão judicial fundamentada (...)" (sic), o que teria sido positivado no art. 2º da Lei nº 9.296/96.

Destaca também que o Conselho Nacional de Justiça editou a Resolução nº 59/2008 para tratar da interceptação telefônica e telemática, "(...) explicitando a necessidade de indicação: (i) dos indícios razoáveis de autoria ou participação dos alvos nos crimes investigados; (ii) das diligências anteriormente realizadas; e (iii) dos motivos que embasam a conclusão de que seria impossível obter a prova por outra via. A Resolução veda, ainda, *"a interceptação de outros números não discriminados na decisão"*, dentre outras restrições (...)" (sic – destaque no original).

Invoca, outrossim, as disposições contidas nos arts. 3º, 7º, 8º e 22 da Lei nº 12.965/2014 (Marco Civil da Internet), aduzindo que exigem, para a quebra do sigilo de registros de conexão, a existência de indícios de ato ilícito.

Discorrendo sobre a importância da proteção do direito à privacidade, argumenta que, "Do ponto de vista teórico, argumentar com uma possível excepcionalidade do caso seria o mesmo que admitir uma inconstitucionalidade e ilegalidade útil. Do ponto de vista prático, não demoraria para a exceção ser banalizada – ainda mais em contextos de intensa criminalidade" (sic).

Faz considerações a respeito do risco de concessão de medidas genéricas de quebra de sigilos, inclusive quanto à repercussão da competência para o exame de tais requerimentos quando eventualmente envolverem pessoas ocupantes de cargos com prerrogativa de foro.

Defende, por derradeiro, que a medida não atende ao Princípio da Proporcionalidade em todas as suas 03 (três) vertentes, quais sejam, adequação, necessidade e proporcionalidade em sentido estrito.

Postula, em sede liminar, que sejam suspeitos os efeitos do ato impugnado, impedindo, inclusive, a aplicação das sanções fixadas na decisão objeto deste impetração.

A liminar foi indeferida em decisão proferida em 11/05/2018.

O Impetrado prestou as informações juntadas aos autos em 21/05/2018.

Os Impetrantes interpuseram o Agravo Regimental (Interno) nº 201800111901 em 30/05/2018, repetindo as razões já lançadas na petição inicial deste *mandamus*, estando o recurso ainda pendente de julgamento.

Devidamente notificado, o órgão de representação judicial do Estado de Sergipe não se manifestou nos autos, a teor do Ato Ordinatório lançado nos autos em 08/06/2018.

O Procurador-Geral de Justiça José Rony Silva Almeida lançou manifestação nos autos em 20/06/2018 no sentido de aguardar o julgamento do Agravo Regimental interposto nestes autos para se manifestar.

Em 21/06/2018 proferi despacho determinando o retorno dos autos ao *Parquet* para emissão de parecer diante da inexistência de efeito suspensivo no Agravo Regimental e de qualquer outro impeditivo para o prosseguimento do presente *writ*.

Após o decurso do prazo de 10 (dez) dias para manifestação do Procurador-Geral de Justiça, proferi despacho em 14/07/2018 determinando a inclusão do processo em pauta para julgamento.

O Procurador-Geral de Justiça em exercício Eduardo Barreto d´Ávila Fontes lançou parecer em 16/07/2018 opinando pela denegação da ordem, entendo pelo não cabimento do *mandamus* por não revelar manifesta ilegalidade ou abuso de autoridade e, no mérito, pela inexistência do direito líquido e certo alegado.

É o Relatório.

VOTO

Desembargadora Iolanda Santos Guimarães (Relatora): – Trata-se de Mandado de Segurança impetrado pelo *Google Brasil Internet Ltda.* e *Google LLC.* contra ato do *Juízo de Direito da Comarca de Porto da Filha*, o qual teria proferido decisão autorizando a quebra do sigilo telemático de um conjunto de pessoas não identificadas nos autos de Inquérito Policial.

O presente mandado de segurança objetiva anular a decisão que impôs aos Impetrantes o fornecimento, no prazo de 72h (setenta e duas horas), de dados telemáticos (contas, nomes de usuário, números de *IP* que foram usados associados a *smartphones* com sistema *Android*, número de IMEI e e-mail associados aos aparelhos e usuários que recorreram aos serviços dos Impetrantes) das pessoas que passaram por locais determinados em intervalos de tempo definidos, sob pena de prática do crime de desobediência e incidência de multa diária de R$ 50.000,00 (cinquenta mil reais).

Os Impetrantes fundamentam seu pedido sob o fundamento de ter sido deferida em inobservâncias a disposições constitucionais e legais.

Nesse sentido, invocam, inicialmente, o disposto no art. 5º, incisos X e XII, da Constituição Federal, que tutelam o direito à privacidade e ao sigilo das comunicações:

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
>
> (...)
>
> X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;
>
> (...)
>
> XII - 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;
>
> (...)

De fato, a simples leitura dos dispositivo constitucionais transcritos revela que a Carta Política vigente previu, como direito fundamentação, a proteção à privacidade que, a reboque, traz consigo o direito ao sigilo das comunicações.

Especificamente quanto às comunicações, a Lei nº 9.296/96 regulamenta a parte final do inciso XII anteriormente citado, prevendo a possibilidade de serem interceptadas as comunicações telefônicas, conforme previsão do seu art. 1º, possibilidade essa ampliada para os sistemas de informática e telemática no seu parágrafo único:

> Art. 1º A interceptação de comunicações telefônicas, de qualquer natureza, para prova em investigação criminal e em instrução processual penal, observará o disposto nesta Lei e dependerá de ordem do juiz competente da ação principal, sob segredo de justiça.
>
> Parágrafo único. O disposto nesta Lei aplica-se à interceptação do fluxo de comunicações em sistemas de informática e telemática.

Especificamente sobre os dados que transitam pela rede mundial de computadores (*Internet*), a Lei nº 12.965/2014 (marco Civil da Internet) estabeleceu os princípios, garantias, direitos e deveres.

Da leitura de ambos os diplomas legais, pode-se perceber que há uma diferenciação na proteção dada pela legislação quanto ao conteúdo das comunicações

mantidas entre indivíduos e quanto às informações de conexão e de acesso a aplicações de *internet*.

Em relação ao conteúdo das comunicações mantidas entre indivíduos, ambos os diplomas – Leis nºs 9.296/96 e 12.965/2014 – restringem a possibilidade de quebra do sigilo. Exigem, para tanto, que haja decisão judicial, precedida de requerimento de autoridades específicas e em hipóteses limitadas, definidas em ambos os diplomas.

Leia-se, a propósito, o disposto nos arts. 2º a 5º e 9º a 10 da Lei nº 9.296/96:

> Art. 2° 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.
>
> Parágrafo único. Em qualquer hipótese deve ser descrita com clareza a situação objeto da investigação, inclusive com a indicação e qualificação dos investigados, salvo impossibilidade manifesta, devidamente justificada.
>
> Art. 3° A interceptação das comunicações telefônicas poderá ser determinada pelo juiz, de ofício ou a requerimento:
>
> I - da autoridade policial, na investigação criminal;
>
> II - do representante do Ministério Público, na investigação criminal e na instrução processual penal.
>
> Art. 4° O pedido de interceptação de comunicação telefônica conterá a demonstração de que a sua realização é necessária à apuração de infração penal, com indicação dos meios a serem empregados.
>
> § 1° Excepcionalmente, o juiz poderá admitir que o pedido seja formulado verbalmente, desde que estejam presentes os pressupostos que autorizem a interceptação, caso em que a concessão será condicionada à sua redução a termo.
>
> § 2° O juiz, no prazo máximo de vinte e quatro horas, decidirá sobre o pedido.

> Art. 5° A decisão será fundamentada, sob pena de nulidade, indicando também a forma de execução da diligência, que não poderá exceder o prazo de quinze dias, renovável por igual tempo uma vez comprovada a indispensabilidade do meio de prova.
>
> (...)
>
> Art. 9° A gravação que não interessar à prova será inutilizada por decisão judicial, durante o inquérito, a instrução processual ou após esta, em virtude de requerimento do Ministério Público ou da parte interessada.
>
> Parágrafo único. O incidente de inutilização será assistido pelo Ministério Público, sendo facultada a presença do acusado ou de seu representante legal.
>
> Art. 10. Constitui crime realizar interceptação de comunicações telefônicas, de informática ou telemática, ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei.
>
> Pena: reclusão, de dois a quatro anos, e multa.

No mesmo sentido, as previsões dos arts. 7º, incisos I, II, III, VII, VIII, IX, 10, §2º, e 12 da Lei nº 12.965/2014:

> Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
>
> I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação;
>
> 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;
>
> (...)
>
> VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;
>
> VIII - informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que:
>
> a) justifiquem sua coleta;

b) não sejam vedadas pela legislação; e

c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet;

IX - consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais;

(...)

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.

(...)

§ 2º O conteúdo das comunicações privadas somente poderá ser disponibilizado mediante ordem judicial, nas hipóteses e na forma que a lei estabelecer, respeitado o disposto nos incisos II e III do art. 7º.

(...)

Art. 12. Sem prejuízo das demais sanções cíveis, criminais ou administrativas, as infrações às normas previstas nos arts. 10 e 11 ficam sujeitas, conforme o caso, às seguintes sanções, aplicadas de forma isolada ou cumulativa:

I - advertência, com indicação de prazo para adoção de medidas corretivas;

II - multa de até 10% (dez por cento) do faturamento do grupo econômico no Brasil no seu último exercício, excluídos os tributos, considerados a condição econômica do infrator e o princípio da proporcionalidade entre a gravidade da falta e a intensidade da sanção;

III - suspensão temporária das atividades que envolvam os atos previstos no art. 11; ou

IV - proibição de exercício das atividades que envolvam os atos previstos no art. 11.

Parágrafo único. Tratando-se de empresa estrangeira, responde solidariamente pelo pagamento da multa de que trata o caput sua filial, sucursal, escritório ou estabelecimento situado no País.

Por outro lado, ao tratar das informações de conexão e de acesso a aplicações de *internet*, a Lei nº 9.296/96 silencia, prevendo a Lei nº 12.965/2014, a seu turno, a prescindibilidade de decisão judicial em hipóteses específicas. Confira-se,

a propósito, redação de seus arts. 10, §§1º, 3º e 4º, e 22, parágrafo único, do Marco Civil da Internet:

> 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.
>
> (...)
>
> **§ 3º O disposto no caput não impede o acesso aos dados cadastrais que informem qualificação pessoal, filiação e endereço, na forma da lei, pelas autoridades administrativas que detenham competência legal para a sua requisição.**
>
> § 4º As medidas e os procedimentos de segurança e de sigilo devem ser informados pelo responsável pela provisão de serviços de forma clara e atender a padrões definidos em regulamento, respeitado seu direito de confidencialidade quanto a segredos empresariais.
>
> (...)
>
> 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.

A jurisprudência dos Tribunais Superiores já se manifestou nesse sentido. Confira-se, inicialmente, o seguinte precedente do Supremo Tribunal Federal:

> HABEAS CORPUS. NULIDADES: (1) INÉPCIA DA DENÚNCIA; (2) ILICITUDE DA PROVA PRODUZIDA DURANTE O INQUÉRITO POLICIAL; VIOLAÇÃO DE REGISTROS TELEFÔNICOS DO CORRÉU, EXECUTOR DO CRIME, SEM AUTORIZAÇÃO JUDICIAL; (3) ILICITUDE DA PROVA DAS INTERCEPTAÇÕES TELEFÔNICAS DE CONVERSAS DOS ACUSADOS COM ADVOGADOS, PORQUANTO ESSAS GRAVAÇÕES OFENDERIAM O DISPOSTO NO ART. 7º, II, DA LEI 8.906/96, QUE GARANTE O SIGILO DESSAS CONVERSAS. VÍCIOS NÃO CARACTERIZADOS. ORDEM DENEGADA.
>
> (...)
>
> 2. Ilicitude da prova produzida durante o inquérito policial - violação de registros telefônicos de corréu, executor do crime, sem autorização judicial.
>
> 2.1 Suposta ilegalidade decorrente do fato de os policiais, após a prisão em flagrante do corréu, terem realizado a análise dos últimos registros telefônicos dos dois aparelhos celulares apreendidos. Não ocorrência.
>
> 2.2 Não se confundem comunicação telefônica e registros telefônicos, que recebem, inclusive, proteção jurídica distinta. Não se pode interpretar a cláusula do artigo 5º, XII, da CF, no sentido de proteção aos dados enquanto registro, depósito registral. A proteção constitucional é da comunicação de dados e não dos dados. (...)
>
> (...)
>
> 4. Ordem denegada.
>
> (HC 91867, Relator(a): Min. GILMAR MENDES, Segunda Turma, julgado em 24/04/2012, ACÓRDÃO ELETRÔNICO DJe-185 DIVULG 19-09-2012 PUBLIC 20-09-2012)

Do seu inteiro teor, é pertinente destacar a seguinte passagem, *verbis*:

> "Primeiramente, sobreleva destacar que não se confundem *comunicação telefônica* e os *registros telefônicos,* recebendo, inclusive, proteção jurídica distinta*.*
>
> E, como já enfatizei em outras oportunidades, entendo que não se pode interpretar a cláusula do artigo 5º, XII, da CF, no sentido de proteção aos dados enquanto registro, depósito registral. A proteção constitucional *é da comunicação 'de dados' e não os 'dados'.*

O tema foi objeto de percuciente análise em estudo singular desenvolvido por Tércio Sampaio Ferraz. Em síntese, são as seguintes as suas reflexões:

> O sigilo, no inciso XII do art. 5º, está referido à comunicação, no interesse da defesa da privacidade. Isto é feito, no texto, em dois blocos: a Constituição fala em sigilo 'da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas'. Note-se, para a caracterização dos blocos, que a conjunção e une correspondência com telegrafia, segue-se uma vírgula e, depois, a conjunção de dados com comunicações telefônicas. Há uma simetria nos dois blocos. Obviamente o que se regula é comunicação por correspondência e telegrafia, comunicação de dados e telefônica. O que fere a liberdade de omitir pensamento é, pois, entrar na comunicação alheia, fazendo com que o que devia ficar entre sujeitos que se comunicam privadamente passe ilegitimamente ao domínio de um terceiro. Se alguém elabora para si um cadastro sobre certas pessoas, com informações marcadas por avaliações negativas, e o torna público, poderá estar cometendo difamação, mas não quebra sigilo de dados. Se estes dados, armazenados eletronicamente, são transmitidos, privadamente, a um parceiro, em relações mercadológicas, para defesa do mercado, também não está havendo quebra de sigilo. Mas, se alguém entra nesta transmissão como um terceiro que nada tem a ver com a relação comunicativa, ou por ato próprio ou porque uma das partes lhe cede o acesso indevidamente, estará violado o sigilo de dados. A distinção é decisiva: o objeto protegido no direito à inviolabilidade do sigilo não são os dados em si, mas a sua comunicação restringida (liberdade de negação). A troca de informações (comunicação) privativa é que não pode ser violada por sujeito estranho à comunicação. (Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado, Cadernos de Direito Constitucional e Ciência Política, São Paulo, Revista dos Tribunais, n. 1, p. 77-82, 1992; e Revista da Faculdade de Direito da Universidade de São Paulo, v. 88, p. 447, 1993)". (sic – destaques no original)

O Superior Tribunal de Justiça segue a mesma linha de entendimento:

> RECURSO ORDINÁRIO EM HABEAS CORPUS. QUADRILHA. DENÚNCIAS ANÔNIMAS IMPUTANDO A PRÁTICA DE ILÍCITOS. REALIZAÇÃO DE DILIGÊNCIAS PRELIMINARES PARA A APURAÇÃO DA VERACIDADE DAS INFORMAÇÕES. CONSTRANGIMENTO INEXISTENTE.
>
> (...)
>
> NULIDADE DA DECISÃO QUE PERMITIU O ACESSO AOS DADOS CADASTRAIS, HISTÓRICO E EXTRATOS DE CHAMADA TELEFÔNICOS. INAPLICABILIDADE DA LEI 9.296/1996. PROVIMENTO JUDICIAL FUNDAMENTADO. MÁCULA NÃO CONFIGURADA.

1. De acordo com a jurisprudência pacífica desta Corte Superior de Justiça, a quebra do sigilo de dados telefônicos, consistentes no histórico de chamadas, dados cadastrais e extratos de ligações, não se submete à disciplina da Lei 9.296/1996, que trata da interceptação das comunicações telefônicas.

(...)

3. Recurso desprovido.

(RHC 53.541/RJ, Rel. Ministro JORGE MUSSI, QUINTA TURMA, julgado em 12/09/2017, DJe 20/09/2017)

PROCESSO PENAL. HABEAS CORPUS. ROUBO MAJORADO. (1) IMPETRAÇÃO COMO SUCEDÂNEO RECURSAL. IMPROPRIEDADE DA VIA ELEITA. (2) QUEBRA DO SIGILO TELEFÔNICO. PROVIDÊNCIA QUE NÃO SE CONFUNDE COM A INTERCEPTAÇÃO TELEFÔNICA. MOTIVAÇÃO DA MEDIDA. OCORRÊNCIA.

ILEGALIDADADE. NÃO RECONHECIMENTO.

(...)

2. Não se confundem as medidas de quebra de sigilo telefônico com a interceptação de comunicação telefônica, esta última albergada, ademais, pela cláusula de reserva de jurisdição. Daí, não são exigíveis, no contexto da quebra de sigilo de dados, todas as cautelas insertas na Lei 9.296/1996. In casu, o magistrado, em cumprimento do inciso IX do artigo 93 da Constituição da República, motivou a quebra do sigilo de dados, com base na intensa utilização de certo terminal telefônico, havendo a franca possibilidade de se desvendar, com base em dados cadastrais oriundos das registros de companhia telefônica, a autoria de um quarto agente no concerto delitivo.

3. Ordem não conhecida.

(HC 237.006/DF, Rel. Ministra MARIA THEREZA DE ASSIS MOURA, SEXTA TURMA, julgado em 27/06/2014, DJe 04/08/2014)

No presente caso, conforme fora bem destacado pela Autoridade Policial em seu requerimento, a solicitação direcionada aos Impetrantes se limitou 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 aos aparelhos e usuários que recorreram aos serviços dos Impetrantes).

Não há qualquer pedido de quebra do sigilo do conteúdo das comunicações eventualmente transmitidas pelos indivíduos a serem atingidos pela medida excepcional.

Como já explicado anteriormente, não se tratando de conteúdo de conversas ou outras formas de comunicação telefônicas ou telemáticas, as hipóteses

que a legislação autoriza a quebra do sigilo são mais amplas, estando previstas no art. 22 do Marco Civil da Internet.

Partindo-se dessa premissa, verifica-se que os requisitos contidos nos 03 (três) incisos do dispositivo legal citado se acham presentes.

Com efeito, trata-se de Inquérito Policial em que se investiga o brutal homicídio perpetrado contra 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 SE-200, no Município de Porto da Folha/SE.

A existência de ilícito, inclusive de natureza criminal, é evidente, restando preenchida a exigência do art. 22, inciso I, do Marco Civil da Internet.

Em relação ao inciso II do art. 22 daquele diploma legal, a representação formulada pela Autoridade Policial reportou exaustivamente a necessidade da medida para o prosseguimento das investigações, especialmente a fim de ser possível a identificação dos indivíduos que cometeram o crime hediondo.

Finalmente, a Autoridade Policial limitou as áreas e os períodos de tempo dos registros dos dados necessários às investigações.

A esse respeito, é preciso destacar e reforçar que, não obstante a medida realmente possa atingir pessoas que não possuem qualquer pertinência com os fatos investigados, **a intimidade delas não será fragilizada em razão de os dados requeridos se limitarem à identificação dos equipamentos eletrônicos eventualmente utilizados naquelas regiões e naqueles intervalos de tempo, não se adentrando no conteúdo de possíveis comunicações que partiram daquelas localidades**.

Em relação a este aspecto em específico, vale citar também as informações prestadas pela Autoridade Impetrada, *in verbis*:

> "Ressalta-se que na forma declinada na decisão datada de 27/04/2018, a decisão não atinge o número indeterminados de usuários, mas apenas aqueles que utilizaram-se dos serviços, nas coordenadas geográficas e no tempo indicado, ou seja, abrangido entre 04 de abril de 2018 às 22h40min e 04 de abril de 2018 às 22h55m, ou seja, são apenas 15 minutos.
>
> Por fim, o local das coordenadas geográficas indicadas não é um centro urbano, onde de fato, haveria um número indeterminado de pessoas circulando. Muito pelo contrário, o local indicado nas coordenadas, trata-se de local ermo, estrada de difícil acesso, de restrita circulação de pessoas, especialmente no horário indicado, motivo pelo qual a alegação das impetrantes de violação de suposta a número indiscriminado de pessoas, não se aplica ao caso em tela, ressalvando-se não existe direito individual absoluto, considerando a própria autorização constitucional (art. 5º inciso XII da CF), e não cabem as partes impetrantes, eventualmente, em nome próprio defender interesse alheio". (sic)

Vale dizer também, por derradeiro, que as razões recursais lançadas no Agravo Regimental interposto pelos Impetrantes não trazem nenhum argumento novo, passível de alterar as considerações já feitas quando da apreciação da liminar ou mesmo de alterar o entendimento ora exposto no julgamento do mérito deste *writ*.

Por todo o exposto, conheço do mandado de segurança, mas para denegar a ordem pleiteada.

Custas pelos Impetrantes, observando-se a isenção do ônus referente a honorários advocatícios, nos termos da Súmula 512 do STF.

É como voto.

Aracaju/SE, 22 de Agosto de 2018.

DESA. IOLANDA SANTOS GUIMARÃES
RELATOR
VOTO VENCIDO

Na Sessão do dia 22.08.2018, restei vencido por acompanhar o voto do Desembargador **Ricardo Múcio Santana de Abreu Lima**, cujas razões foram assim lançadas:

> "Entendo que a quebra do sigilo é medida excepcional que só pode ser deflagrada com a existência de indícios concretos de atividade ilícita por parte do alvo, a ser demonstrados em decisão judicial fundamentada.
>
> O Conselho Nacional de Justiça editou a Resolução nº 59/2008 e regulou a interceptação telefônica e telemática exigindo requisitos dentre os quais se insere a necessidade de indicação, os indícios razoáveis da autoria ou participação em infração criminal apenada com reclusão; as diligências anteriormente realizadas e os motivos que embasam a conclusão de que seria impossível obter a prova por outra via.
>
> No caso dos autos, entendo que tais requisitos não foram cumpridos e, principalmente, expresso meu raciocínio no sentido de que a interceptação telemática foi genérica e ofenderá a todos os munícipes, sem discriminação. A interceptação requerida seria realizada em uma rodovia, sem indicar nomes ou pessoas.
>
> O fato é que a interceptação só pode ser realizada quando ela é aliada a presença de indícios de autoria e quando já foram exauridos outros meios comuns de prova.
>
> 'PROCESSUAL PENAL - HABEAS CORPUS - OPERAÇÃO DILÚVIO DA POLÍCIA FEDERAL - DESCAMINHO - FALSIDADE IDEOLÓGICA - LAVAGEM DE DINHEIRO - INTERCEPTAÇÃO TELEMÁTICA DE DADOS - INDÍCIOS DE AUTORIA - IMPOSSIBILIDADE DE PROVAR POR OUTROS MEIOS - ELEMENTOS DE PROVA OBTIDOS POR MEIO LÍCITO - AUSÊNCIA DE CONSTRANGIMENTO ILEGAL - ORDEM DENEGADA.
>
> 1. A interceptação telemática anterior a que se questiona, realizada com autorização judicial em relação a co-réu, constitui elemento idôneo a caracterizar os indícios de autoria necessários à quebra do sigilo telemático de outra pessoa suspeita, no curso da investigação policial.
>
> **2. Inexiste ilegalidade na interceptação telemática realizada quando ela é, aliada a presença de indícios de autoria, devido a peculiaridade do *modus operandi* do delito, o único meio de prova a esclarecer os fatos.**

3. É idônea a fundamentação da decisão que esclarece a existência de indícios de autoria a possibilitar a quebra do sigilo telemático, ainda que a fundamentação seja sucinta.

4. Ordem denegada.

(STJ - HC: 101165 PR 2008/0045469-8, Relator: Ministra JANE SILVA (DESEMBARGADORA CONVOCADA DO TJ/MG), Data de Julgamento: 01/04/2008, T6 - SEXTA TURMA, Data de Publicação: DJe 22/04/2008)'

A decisão, como proferida, fere a liberdade e a intimidade das pessoas que por ali transitam e serão abrangidas pela investigação, violando a Constituição Federal.

Em caso similar, o STJ afirmou que '***é exigida não só para a decisão que defere a interceptação telefônica, como também para as sucessivas prorrogações, a concreta indicação dos requisitos legais de justa causa e imprescindibilidade da prova, que por outros meios não pudesse ser feita.'***

'(...)

1. É exigida não só para a decisão que defere a interceptação telefônica, como também para as sucessivas prorrogações, a concreta indicação dos requisitos legais de justa causa e imprescindibilidade da prova, que por outros meios não pudesse ser feita.

.....

3. Recurso especial provido para declarar nula a decisão inicial de quebra do sigilo telefônico e as sucessivas prorrogações e, bem assim, das provas consequentes, a serem aferidas pelo magistrado na origem, devendo o material respectivo ser extraído dos autos, procedendo-se à prolação de nova sentença com base nas provas remanescentes, estendido seus efeitos aos demais corréus, ficando prejudicadas as demais questões arguidas nos agravos e recursos especiais.

(REsp 1670637/SP, Rel. Ministro NEFI CORDEIRO, SEXTA TURMA, julgado em 13/03/2018, DJe 03/04/2018)'

Com esses fundamentos, VOTO pela **CONCESSÃO** da segurança.

É como voto."

Portanto, tendo em vista haver acompanhado integralmente as argumentações do eminente colega, ficam estas expressando o meu voto.

É como voto.

Aracaju/SE, 22 de Agosto de 2018.

DES. RUY PINHEIRO DA SILVA

VOTO VENCIDO

Trata-se de mandado de segurança impetrado pela GOOGLE BRASIL INTERNET LTDA e GOOGLE LLC contra ato do Juízo de Direito da Comarca de Porto da Folha que deferiu o Pedido de Quebra de Sigilo de Dados e/ou telefônico nº 0000555-28.2018.8.25.0062, inquérito policial formalizado no âmbito de

investigação conduzida pela Divisão de Inteligência e Planejamento Policial (DIPOL) do Centro de Operações Policiais Especiais (COPE) da polícia civil de Sergipe, que apura um crime de homicídio.

Na última sessão do Pleno do dia 08/08/2018, após a sustentação oral do advogado dos impetrantes, houve manifestação de alguns dos Eminentes colegas, com discussões sobre interceptação telefônica e de dados telemáticos, suas diferenças, abrindo a divergência o Desembargador Ricardo Múcio, com fortes argumentos que me instigaram a pedir vista dos autos para melhor exame da matéria.

A decisão impugnada pelo presente *writ* foi exarada no processo de **nº 201880000590**, disponibilizada no diário eletrônico deste Tribunal no dia **06/04/2018**, cuja parte dispositiva está redigida nos seguintes termos:

"Com essas razões, acolho o pedido formulado pela autoridade policial, e, com esteio no art. 5º, inc. XII, da Constituição Federal, bem assim em face do art. 1º c/c arts. 3º, inc. I e 5º, ambos da Lei nº 9.296/96 DEFIRO o pedido de Quebra do Sigilo de Dados Telefônicos e Interceptação Telefônica nos termos r e q u e r i d o s . Fixo às operadoras de telefonia o prazo de 05 (cinco) dias para o início do cumprimento desta decisão, sob pena da prática do crime de desobediência pelos encarregados. Encaminhem-se as informações acima determinadas à Divisão de Inteligência e Planejamento Policial – D I P O L , e m n o m e d o A g e n t e P o l i c i a l i n d i c a d o . Expeçam-se os competentes Alvarás, entregando-os à autoridade policial ou pessoa sob seus cuidados, m e d i a n t e c e r t i d ã o n o s a u t o s ."

O eminente magistrado assinou alvará de **quebra de sigilo de dados telemáticos** com o detalhamento da sua determinação, de modo a exigir que fossem informadas as contas e nomes de usuário (username) e todos os números de IP (registro de conexão), além do número do IMEI e email associados aos aparelhos e usuários que recorreram aos serviços da companhia, em um raio de 500 metros das coordenadas geográficas ali especificadas, no período abrangido entre às 22h40min e 22h55min do dia 04/04/2018.

Aqui reside o **ponto central de questionamento** das impetrantes, qual seja, na determinação da quebra do sigilo telemático de um conjunto não identificado de pessoas, unidas tão somente pela circunstância aleatória de terem transitado por determinadas coordenadas geográficas, em certo lapso de tempo.

A lei nº 9.296/96, indicada na decisão, tem por objeto a regulamentação do inciso XII, parte final, do art. 5º da Constituição Federal, consoante dispõe sua ementa. O referido dispositivo constitucional está redigido nos seguintes termos:

"*XII – 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."*

Na delimitação do legislador constituinte, sendo inviolável o sigilo de dados e das comunicações telefônicas, a quebra desta regra é medida excepcional, submetida à reserva de jurisdição, sob a disciplina da lei.

A lei 9.296/96 possibilita a interceptação de comunicações telefônicas de qualquer natureza, como bem leciona o aclamado processualista RENATO BRASILEIRO:

"Considerando o fantástico desenvolvimento da informática na atualidade, a expressão comunicação telefônica não deve se restringir às comunicações por telefone. Por força de interpretação progressiva, a expressão comunicação telefônica deve também abranger a transmissão, emissão ou recepção de símbolos, caracteres, sinais, escritos, imagens, sons ou informações de qualquer natureza, por meio de telefonia, estática, ou móvel (celular). Por conseguinte, é possível a interceptação de qualquer comunicação via telefone, conjugada ou não com a informática, o que compreende aquelas realizadas direta (fax, modens) e indiretamente (internet, e-mail, correios eletrônicos).

*Daí dispor o caput do art. 1º da Lei nº 9.296/96 ser possível a interceptação de comunicações telefônicas de **qualquer natureza**, acrescentando o parágrafo único do mesmo artigo que o disposto nesta Lei aplica-se à interceptação do fluxo de comunicações em sistemas de informática e telemática. Por telemática compreende-se a ciência que cuida da comunicação (transmissão, manipulação) de dados, sinais, imagens, escritos e informações por meio do uso combinado da informática (do computador) com as váris formas de telecomunicação, ou seja, telemática é a telecomunicação associada à informática.*

*[...] a nosso juízo, quando a Constituição Federal autoriza a **interceptação das comunicações telefônicas**, refere-se não só as comunicações telefônicas propriamente ditas como também à comunicação de dados, imagens e sinais através da telemática."* (in Manual de Processo Penal . Volume único. 2ª edição. 2014. Salvador. Editora Juspodivm. Pg 701/702.)

Exatamente o caso em exame, onde a autoridade impetrada, ao acolher pedido formulado pela autoridade policial, deferiu a quebra de sigilo de dados telemáticos

Contudo, há de se ressaltar que, independentemente da modalidade de interceptação autorizada como medida cautelar, a Lei 9.296/96 impõe rígidos requisitos e proibições de modo a não vulnerar direito fundamental à intimidade privada (inciso X, do art. 5º da CR/88).

Merece destaque o seguinte dispositivo:

"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.

Parágrafo único. Em qualquer hipótese deve ser descrita com clareza a situação objeto da investigação, inclusive com a indicação e qualificação dos investigados, salvo impossibilidade manifesta, devidamente justificada." Grifa-se.

Quanto ao requisito de indícios razoáveis da autoria, ressalta o professor RENATO BRASILEIRO:

"Se a lei demanda a presença de indícios razoáveis de autoria ou participação em infração penal (Lei nº 9.296/96, art. 2º, I), uma simples manifestação policial ou ministerial, por si sós, não autorizam a decretação da interceptação telefônica. É necessário que a representação da autoridade policial ou o requerimento do Ministério Público estejam acompanhados de mais dados, de elementos informativos ou de provas já obtidas, que possibilitem ao juiz formar sua convicção.

Complementando o quanto previsto no art. 2º, inciso I, da Lei nº 9.296/96, o parágrafo único do mesmo dispositivo prevê que, em qualquer hipótese, deve ser descrita com clareza a situação objeto da

investigação, inclusive com a indicação e qualificação dos investigados, salvo impossibilidade manifesta, devidamente injustificada.

O parágrafo único do art. 2º da Lei nº 9.296/96 permite concluir que, caso a Polícia tenha conhecimento da prática de determinado delito, mas ainda não possua um suspeito, será possível a decretação de interceptação telefônica sobre pessoa indeterminada, objetivando descobrir-se o provável autor ou partícipe do fato delituoso, hipótese em que a diligência deverá recair sobre uma determinada linha telefônica, a ser individualizada no pedido." (ob. Cit. Pg. 713)."

Portanto, Eminentes Colegas, a doutrina orienta, ao interpretar a teleologia da regra legal de quebra de dados, a necessidade de individualização de quem será investigado, fundada em razoáveis indícios de autoria. A partir desta perspectiva, ressoa irrazoável a interceptação difusa de pessoas, sem declinar nomes e os respectivos motivos de estarem como objeto de investigação, sem demonstração de qualquer vínculo indiciário concreto entre os investigados.

O ordenamento jurídico brasileiro exige seja demonstrado, na fundamentação da decisão de quebra de dados telemáticos, um liame mínimo, razoável, entre o fato criminoso e um ou alguns sujeitos determinados, de modo a legitimar a sujeição dos mesmos como alvos de investigação. A utilização do critério exclusivamente geográfico/temporal, recaindo difusamente sobre pessoas indeterminadas, de forma genérica, não está albergada pela legislação pátria.

O STF já examinou casos similares onde rechaçou pedidos de quebra com base em coordenadas geográficas, alcançando pessoas que não seriam partes do processo. Destaque-se o seguinte trecho da decisão da lavra da Ministra Carmen Lúcia no **HC131538**:

"Por fim, o requerimento da quebra de sigilo telefônico de algumas Estações Rádio Bases (ERB's) no período compreendido entre as 08:OOhs do dia 01/07/2012 e 24:00hs do dia 05/07/2012, igualmente, mostra-se desarrazoado.

Conforme asseverou o magistrado singular, além da providência pleiteada alcançar uma infinidade de usuários sem nenhuma ligação com o processo, na quebra do sigilo telefônico dos processados encontram-se as respectivas ERB's referentes aos números por eles utilizados durante o dia 05/07/2012, data do delito."

Na mesma linha, o entendimento do STJ, ao deferir o pedido de tutela provisória **interposto pelo GOOGLE BRASIL INTERNET LTDA e GOOGLE INC., no RMS 54.133/SP,** contra acórdão do Tribunal de Justiça do Estado de São Paulo, tendo o Ministro Antonio Saldanha Palheiro ressaltado o seguinte:

"Nada obstante, a GOOGLE BRASIL INTERNET LTDA. e GOOGLE INC. se insurgiram contra o citado acórdão, mediante a interposição de recurso ordinário em mandado de segurança, cuja cópia encontra-se acostada às e-STJ fls. 54/88, em que alertaram a existência de patente periculum in mora, pois mantida a ordem judicial determinando a quebra do sigilo de dados telemáticos, com possível submissão a penalidades, além da presença do fumus boni iuris, derivado do acervo probatório colacionado nesta Tutela Provisória, que denotaria o possível risco de violação à esfera privada dos usuários da plataforma Android que tenham transitado pelo referido espaço geográfico.

Assim, gizadas as circunstâncias que revolvem o caso em apreço, tenho por caracterizada a presença da probabilidade do direito, considerando, ainda, que houve interposição do recurso ordinário em mandado de segurança (RMS 54.133/SP).

O perigo da demora decorre do próprio comando judicial, visto que a manutenção do descumprimento da referida ordem submete as requerentes às sanções cabíveis."Grifa-se.

Como se não bastassem todos estes argumentos, o CONSELHO NACIONAL DE JUSTIÇA (CNJ), editou recentemente a **Resolução 217, de 16/02/2016**, alterando e acrescentando dispositivos à **Resolução nº 59, de 09/09/2008,** que disciplina e uniformiza as rotinas visando ao aperfeiçoamento do

procedimento de interceptação de comunicações telefônicas e de sistema de informática e telemática nos órgãos jurisdicionais do Poder Judiciário, a que se refere a Lei 9.296, de 24/07/1996.

Assim, vejamos a atual redação da normatização do CNJ sobre as medidas cautelares em interceptações:

*"**DO DEFERIMENTO DA MEDIDA CAUTELAR DE INTERCEPTAÇÃO***

Art. 10. Atendidos os requisitos legalmente previstos para deferimento da medida, o Magistrado fará constar expressamente em sua decisão:

I - a autoridade requerente;

II - o relatório circunstanciado da autoridade requerente;

III - os indícios razoáveis da autoria ou participação em infração criminal apenada com reclusão;

IV - as diligências preparatórias realizadas, com destaque para os trabalhos mínimos de campo, com exceção de casos urgentes, devidamente justificados, em que as medidas iniciais de investigação sejam inviáveis;

V - os motivos pelos quais não seria possível obter a prova por outros meios disponíveis;

VI - os números dos telefones ou o nome de usuário, e-mail ou outro identificador no caso de interceptação de dados;

VII - o prazo da interceptação, consoante o disposto no art. 5º da Lei 9.296/1996;

VIII - a imediata indicação dos titulares dos referidos números ou, excepcionalmente, no prazo de 48 (quarenta e oito) horas;

IX - a expressa vedação de interceptação de outros números não discriminados na decisão;

X - os nomes de autoridades policiais e de membros do Ministério Público responsáveis pela investigação, que terão acesso às informações;

XI - os nomes dos servidores do cartório ou da secretaria, bem assim, se for o caso, de peritos, tradutores e demais técnicos responsáveis pela tramitação da medida e expedição dos respectivos ofícios, no Poder Judiciário, na Polícia Judiciária e no Ministério Público, podendo reportar-se à portaria do juízo que discipline a rotina cartorária.

§ 1º Nos casos de formulação de pedido verbal de interceptação (art. 4º, § 1º, da Lei 9.296/1996), o servidor autorizado pelo magistrado deverá reduzir a termo os pressupostos que autorizem a interceptação, tais como expostos pela autoridade policial ou pelo representante do Ministério Público.

§ 2º A decisão judicial será sempre escrita e fundamentada.

§ 3º Fica vedada a utilização de dados ou informações que não tenham sido legitimamente gravados ou transcritos."

Portanto, Eminentes Colegas, chamo a atenção para a intensificação do rigor que recai sobre o exame dos requisitos para o deferimento das interceptações, como medida cautelar, de modo a evitar exatamente os excessos que possam invadir a esfera privada de terceiros, alheios aos fatos objeto de investigação.

A justificativa apresentada pela autoridade impetrada, cujo trecho foi destacado pela Eminente Relatora, em nada justifica ou demonstra a identificação dos investigados à luz da legislação vigente, pois só reitera a suficiência da delimitação geográfico-temporal como critério delimitador legítimo para a investigação.

Ao revés, suas justificativas não se mostram aptas a elidir os vícios alegados pelos impetrantes relativos a inconstitucionalidade e ilegalidade da determinação de quebra de dados telemáticos de forma difusa, sem especificação dos investigados, como exige o ordenamento jurídico, de modo a evitar o risco de que terceiros sejam alcançados, e violados em sua intimidade privada, mesmo sem qualquer relação com o fato criminoso.

Assim, e firme em tais fundamentos, acompanho a divergência e voto pela concessão da segurança.

É como voto.

Aracaju/SE, 22 de Agosto de 2018.

DES. ALBERTO ROMEU GOUVEIA LEITE

Trata-se de Mandado de Segurança impetrado pelo Google Brasil Internet Ltda. e Google LLC. contra ato do Juízo de Direito da Comarca de Porto da Filha, o qual teria proferido decisão autorizando a quebra do sigilo telemático de um conjunto de pessoas não identificadas nos autos de Inquérito Policial.

Os Impetrantes defendem ser inconstitucional e ilegal a medida determinada pela Autoridade Impetrada, invocando o teor do art. 5º, incisos X e XII, da Constituição Federal, que protegem o direito à privacidade e das comunicações, destacando, ainda, o disposto no art. 93, inciso IX, da CF/88 para apontar a ausência de fundamentação específica na decisão questionada.

É o Relatório.

Entendo que a quebra do sigilo é medida excepcional que só pode ser deflagrada com a existência de indícios concretos de atividade ilícita por parte do alvo, a ser demonstrados em decisão judicial fundamentada.

O Conselho Nacional de Justiça editou a Resolução nº 59/2008 e regulou a interceptação telefônica e telemática exigindo requisitos dentre os quais se insere a necessidade de indicação, os indícios razoáveis da autoria ou participação em infração criminal apenada com reclusão; as diligências anteriormente realizadas e os motivos que embasam a conclusão de que seria impossível obter a prova por outra via.

No caso dos autos, entendo que tais requisitos não foram cumpridos e, principalmente, expresso meu raciocínio no sentido de que a interceptação telemática foi genérica e ofenderá a todos os munícipes, sem discriminação. A interceptação requerida seria realizada em uma rodovia, sem indicar nomes ou pessoas.

O fato é que a interceptação só pode ser realizada quando ela é aliada a presença de indícios de autoria e quando já foram exauridos outros meios comuns de prova.

‘PROCESSUAL PENAL - HABEAS CORPUS - OPERAÇÃO DILÚVIO DA POLÍCIA FEDERAL - DESCAMINHO - FALSIDADE IDEOLÓGICA - LAVAGEM DE DINHEIRO - INTERCEPTAÇÃO TELEMÁTICA DE DADOS -

INDÍCIOS DE AUTORIA - IMPOSSIBILIDADE DE PROVAR POR OUTROS MEIOS - ELEMENTOS DE PROVA OBTIDOS POR MEIO LÍCITO - AUSÊNCIA DE CONSTRANGIMENTO ILEGAL - ORDEM DENEGADA.

1. A interceptação telemática anterior a que se questiona, realizada com autorização judicial em relação a co-réu, constitui elemento idôneo a caracterizar os indícios de autoria necessários à quebra do sigilo telemático de outra pessoa suspeita, no curso da investigação policial.

2. Inexiste ilegalidade na interceptação telemática realizada quando ela é, aliada a presença de indícios de autoria, devido a peculiaridade do *modus operandi* do delito, o único meio de prova a esclarecer os fatos.

3. É idônea a fundamentação da decisão que esclarece a existência de indícios de autoria a possibilitar a quebra do sigilo telemático, ainda que a fundamentação seja sucinta.

4. Ordem denegada.

(STJ - HC: 101165 PR 2008/0045469-8, Relator: Ministra JANE SILVA (DESEMBARGADORA CONVOCADA DO TJ/MG), Data de Julgamento: 01/04/2008, T6 - SEXTA TURMA, Data de Publicação: DJe 22/04/2008)'

A decisão, como proferida, fere a liberdade e a intimidade das pessoas que por ali transitam e serão abrangidas pela investigação, violando a Constituição Federal.

Em caso similar, o STJ afirmou que '***é exigida não só para a decisão que defere a interceptação telefônica, como também para as sucessivas prorrogações, a concreta indicação dos requisitos legais de justa causa e imprescindibilidade da prova, que por outros meios não pudesse ser feita.'***

'(...)

1. É exigida não só para a decisão que defere a interceptação telefônica, como também para as sucessivas prorrogações, a concreta indicação dos requisitos legais de justa causa e imprescindibilidade da prova, que por outros meios não pudesse ser feita.

.....

3. Recurso especial provido para declarar nula a decisão inicial de quebra do sigilo telefônico e as sucessivas prorrogações e, bem assim, das provas consequentes, a serem aferidas pelo magistrado na origem, devendo o material respectivo ser extraído dos autos, procedendo-se à prolação de nova sentença com base nas provas remanescentes, estendido seus efeitos aos demais corréus, ficando prejudicadas as demais questões arguidas nos agravos e recursos especiais.

(REsp 1670637/SP, Rel. Ministro NEFI CORDEIRO, SEXTA TURMA, julgado em 13/03/2018, DJe 03/04/2018)'

Com esses fundamentos, VOTO pela **CONCESSÃO** da segurança.

É como voto.

Aracaju/SE, 22 de Agosto de 2018.

DES. RICARDO MÚCIO SANTANA DE A. LIMA