Plenário Virtual

DIREITO CONSTITUCIONAL. DIREITO PROCESSUAL PENAL. QUEBRA DE SIGILO DE DADOS PESSOAIS. REGISTROS DE ACESSO À INTERNET E FORNECIMENTO DE IP. DECISÃO GENÉRICA. NÃO INDICAÇÃO DE PARÂMETROS MÍNIMOS PARA IDENTIFICAÇÃO DOS USUÁRIOS. NÃO DELIMITAÇÃO, ADEMAIS, DO ESPAÇO TERRITORIAL EM QUE VEICULADA A ORDEM. PROTEÇÃO À INTIMIDADE E AO SIGILO DE DADOS (ART. 5º, X e XII, CF). QUESTÃO CONSTITUCIONAL. POTENCIAL MULTIPLICADOR DA CONTROVÉRSIA. REPERCUSSÃO GERAL RECONHECIDA.

Manifestação da Senhora Ministra Rosa Weber: Trata-se de recurso extraordinário interposto, com fundamento no art. 102, III, a, da Constituição Federal, pela Google Brasil Internet Ltda. e pela Google LLC contra acórdão do Superior Tribunal de Justiça que negou provimento a recurso ordinário em mandado de segurança.

Na origem, a impetração das recorrentes, perante o Tribunal de Justiça do Estado do Rio de Janeiro, volta-se contra ato emanado do Juízo de Direito da 4ª Vara Criminal da Comarca da Capital/RJ que determinara às duas empresas o fornecimento da identificação dos IP's ou "DEVICE IDs" que tenham se utilizado do Google Busca (seja através do aplicativo ou sua versão WEB) no período compreendido entre o dia 10/03/2018 a 14/03/2018, para realizar consultas dos seguintes parâmetros de pesquisa: ''MARIELE FRANCO; "VEREADORA MARIELE"; "AGENDA VEREADORA MARIELE; "CASA DAS PRETAS"; "RUA DOS INVÁLIDOS, 122" ou "RUA DOS INVALIDOS".

O Tribunal de Justiça local, por maioria, denegara a segurança, em acórdão assim ementado:

Mandado de Segurança. Decisão decretou no curso de investigação criminal, entre outras medidas, a quebra de sigilo telemático de um conjunto não identificado de pessoas. Alegação de que o ato combatido, nesse item específico, seria genérico e aleatório, além de carente de base constitucional e legal, violando direitos constitucionais e legais, mais especificamente os previstos no artigo 5.º, incisos X, XII, LVII e LIV, da Constituição da República. Direitos à privacidade e ao sigilo de dados que, por não serem absolutos, podem ser relativizados em hipóteses excepcionais, dentre as quais a de investigação criminal. Trata-se de inquérito policial instaurado a fim de apurar a prática, a autoria e a materialidade de dois homicídios qualificados e um homicídio tentado. Crimes graves e de grande repercussão. Não há ilegalidade na decisão motivada, eis que a Constituição da Republica prevê expressamente, em seu artigo 5º, inciso XII, a possibilidade da quebra de sigilo de dados, por ordem judicial, desde que fundamentada. A Lei n.º 9.296/96, artigo 2.º, parágrafo único, permite a não indicação e qualificação dos investigados. Ausência de direito líquido e certo das Impetrantes. Denegação da segurança.

Na sequência, as impetrantes, insatisfeitas com o provimento jurisdicional, interpuseram, com fundamento no art. 105, II, b, da Constituição da República, recurso ordinário em mandado de segurança. O Superior Tribunal de Justiça, por sua vez, como adiantei, negou provimento ao recurso. Colho a ementa do acórdão ora impugnado:

RECURSO EM MANDADO DE SEGURANÇA. DIREITO À PRIVACIDADE E À INTIMIDADE. DETERMINAÇÃO DE QUEBRA DO SIGILO DO REGISTRO DE ACESSO À INTERNET. FORNECIMENTO DE IPS. DETERMINAÇÃO QUE NÃO INDICA PESSOA INDIVIDUALIZADA. AUSÊNCIA DE ILEGALIDADE OU DE VIOLAÇÃO DOS PRINCÍPIOS E GARANTIAS CONSTITUCIONAIS. FUNDAMENTAÇÃO DA MEDIDA. OBSERVÂNCIA. PROPORCIONALIDADE

CONSTITUCIONAIS. FUNDAMENTAÇÃO DA MEDIDA. OCORRÊNCIA. PROPORCIONALIDADE. RECURSO EM MANDADO DE SEGURANÇA NÃO PROVIDO.

1. Os direitos à vida privada e à intimidade fazem parte do núcleo de direitos relacionados às liberdades individuais, sendo, portanto, protegidos em diversos países e em praticamente todos os documentos importantes de tutela dos direitos humanos. No Brasil, a Constituição Federal, no art. 5°, X, estabelece que: "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". A ideia de sigilo expressa verdadeiro direito da personalidade, notadamente porque se traduz em garantia constitucional de inviolabilidade dos dados e informações inerentes a pessoa, advindas também de suas relações no âmbito digital.

2. Mesmo com tal característica, o direito ao sigilo não possui, na compreensão da jurisprudência pátria, dimensão absoluta. De fato, embora deva ser preservado na sua essência, este Superior Tribunal de Justiça, assim como a Suprema Corte, entende que é possível afastar sua proteção quando presentes circunstâncias que denotem a existência de interesse público relevante, invariavelmente por meio de decisão proferida por autoridade judicial competente, suficientemente fundamentada, na qual se justifique a necessidade da medida para fins de investigação criminal ou de instrução processual criminal, sempre lastreada em indícios que devem ser, em tese, suficientes à configuração de suposta ocorrência de crime sujeito à ação penal pública.

3. Na espécie, a ordem judicial direcionou-se a dados estáticos (registros), relacionados à identificação de aparelhos utilizados por usuários que, de alguma forma, possam ter algum ponto em comum com os fatos objeto de investigação por crimes de homicídio.

4. A determinação do Magistrado de primeiro grau, de quebra de dados informáticos estáticos, relativos a arquivos digitais de registros de conexão ou acesso a aplicações de internet e eventuais dados pessoais a eles vinculados, é absolutamente distinta daquela que ocorre com as interceptações das comunicações, as quais dão acesso ao fluxo de comunicações de dados, isto é, ao conhecimento do conteúdo da comunicação travada com o seu destinatário. Há uma distinção conceitual entre a quebra de sigilo de dados armazenados e a interceptação do fluxo de comunicações. Decerto que o art. 5°, X, da CF/88 garante a inviolabilidade da intimidade e da privacidade, inclusive quando os dados informáticos constarem de banco de dados ou de arquivos virtuais mais sensíveis. Entretanto, o acesso a esses dados registrados ou arquivos virtuais não se confunde com a interceptação das comunicações e, por isso mesmo, a amplitude de proteção não pode ser a mesma.

5. Os dispositivos que se referem às interceptações das comunicações indicados pelos recorrentes não se ajustam ao caso sub examine. Deveras, o procedimento de que trata o art. 2° da Lei n. 9.296/1996, cujas rotinas estão previstas na Resolução n. 59/2008 (com alterações ocorridas em 2016) do CNJ, os quais regulamentam o art. 5°, XII, da CF, não se aplica a procedimento que visa a obter dados pessoais estáticos armazenados em seus servidores e sistemas informatizados de um provedor de serviços de internet. A quebra do sigilo de dados, na hipótese, corresponde à obtenção de registros informáticos existentes ou dados já coletados.

6. Não há como pretender dar uma interpretação extensiva aos referidos dispositivos, de modo a abranger a requisição feita em primeiro grau, porque a ordem é dirigida a um provedor de serviço de conexão ou aplicações de internet, cuja relação é devidamente prevista no Marco Civil da Internet, o

qual não impõe, entre os requisitos para a quebra do sigilo, 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.

7. Os arts. 22 e 23 do Marco Civil da Internet, em complemento ao art. 10, parágrafo único, que tratam especificamente do procedimento de que cuidam os autos, não exigem a indicação ou qualquer elemento de individualização pessoal na decisão judicial. Assim, para que o magistrado possa requisitar dados pessoais armazenados por provedor de serviços de internet, mostra-se satisfatória a indicação dos seguintes elementos previstos na lei: a) indícios da ocorrência do ilícito; b) justificativa da utilidade da requisição; e c) período ao qual se referem os registros. Não é necessário, portanto, que o magistrado fundamente a requisição com indicação da pessoa alvo da investigação, tampouco que justifique a indispensabilidade da medida, ou seja, que a prova da infração não pode ser realizada por outros meios, o que, aliás, seria até, na espécie se houvesse tal obrigatoriedade legal plenamente dedutível da complexidade e da dificuldade de identificação da autoria mediata dos crimes investigados.

8. Logo, a quebra do sigilo de dados armazenados, assim entendida a requisição mediante ordem judicial de registros de conexão e acesso à internet, de forma autônoma ou associada a outros dados pessoais e informações, não obriga a autoridade judiciária a indicar previamente as pessoas que estão sendo investigadas, até porque o objetivo precípuo dessa medida, na expressiva maioria dos casos, é justamente de proporcionar a identificação do usuário do serviço ou do terminal utilizado.

9. Conforme dispõe o art. 93, IX, da CF, "todos os julgamentos dos órgãos do Poder Judiciário serão públicos, e fundamentadas todas as decisões, sob pena de nulidade, podendo a lei limitar a presença, em determinados atos, às próprias partes e a seus advogados, ou somente a estes, em casos nos quais a preservação do direito à intimidade do interessado no sigilo não prejudique o interesse público à informação". Na espécie, tanto os indícios da prática do crime, como a justificativa quanto à utilização da medida e o período ao qual se referem os registros foram minimamente explicitados pelo Magistrado de primeiro grau.

10. Quanto à proporcionalidade da quebra de dados informáticos, ela é adequada, na medida em que serve como mais um instrumento que pode auxiliar na elucidação dos delitos, cuja investigação se arrasta por mais de dois anos, sem que haja uma conclusão definitiva; é necessária, diante da complexidade do caso e da não evidência de outros meios não gravosos para se alcançarem os legítimos fins investigativos; e, por fim, é proporcional em sentido estrito, porque a restrição a direitos fundamentais que dela redundam tendo como finalidade a apuração de crimes dolosos contra a vida, de repercussão internacional não enseja gravame às pessoas eventualmente afetadas, as quais não terão seu sigilo de dados registrais publicizados, os quais, se não constatada sua conexão com o fato investigado, serão descartados.

11. Logo, a ordem judicial para quebra do sigilo dos registros, delimitada por parâmetros de pesquisa em determinada região e por período de tempo, não se mostra medida desproporcional, porquanto, tendo como norte a apuração de gravíssimos crimes cometidos por agentes públicos contra as vidas de três pessoas - mormente a de quem era alvo da emboscada, pessoa dedicada, em sua atividade parlamentar, à defesa dos direitos de minorias que sofrem com a ação desse segmento podre da estrutura estatal fluminense - não impõe risco desmedido à privacidade e à intimidade dos usuários possivelmente atingidos pela diligência questionada.

pela diligência questionada.

12. Recurso em mandado de segurança não provido.

Na presente sede recursal, as recorrentes apontam violação dos arts. 5º, X e XII, e 93, IX, da Carta Fundamental.

No tocante à configuração de repercussão geral, as recorrentes pontuam (i) o potencial multiplicador da controvérsia em inúmeros inquéritos policiais, procedimentos investigatórios criminais e ações penais, (ii) a relevância constitucional do tema acerca da proteção de dados pessoais num momento de crescente informatização e inovações tecnológicas, (iii) o aspecto social e econômico da controvérsia, pois as aplicações de internet e dispositivos tecnológicos que envolvem coleta e uso de dados são utilizados em diversas atividades cotidianas, como empresas tradicionais estão cada vez mais se modernizando e incorporando funcionalidades ligadas ao tratamento de dados,

Para amparar sua pretensão, as recorrentes aduzem a potencialidade de a decisão proferida pelo Juízo de primeiro grau atingir enorme número de pessoas que pesquisaram tais termos com objetivos lícitos, desse modo, a ordem é sobre dados privados de pesquisa, a serem disponibilizados sob a perigosa lógica de perfilamento de pessoas por termos de busca inclusive de inclinações políticas através de dados pessoais', para usar a definição legal.

Nesse sentido, asseveram que a decisão objurgada (i) atinge pessoas inocentes, pois os termos indicados são comuns e envolvem pessoa pública (então Vereadora municipal), projeto social e o nome de uma rua popular na cidade do Rio de Janeiro, (ii) indica lapso temporal demasiadamente longo 96h (noventa e seis horas) aumentando a possibilidade de lesar os direitos de grande número de pessoas inocentes, (iii) carece de fundamentação adequada, apesar dessa imensa generalidade, a ordem, sem indicação concreta dos motivos pelos quais essa diligência seria indispensável para o esclarecimento dos envolvidos na prática criminosa, ou seja, decisão genérica que poderia ser inserida em qualquer outra de quebra de sigilo, sobre qualquer tema.

Destacam que os dados atinentes às pesquisas realizadas em sites na internet são protegidos tanto pela cláusula geral de proteção da intimidade (art. 5º, X, CF), quanto pela norma específica de sigilo de dados (art. 5º, XII, CF). Assim, sendo o mundo cada vez mais digital, defendem que os dados gerados por tais pesquisas se encontram albergados pelo núcleo fundamental do direito à privacidade.

Aduzem não estarem afirmando que o direito à privacidade seria absoluto, mas, segundo alegam, para reconciliação do direito à privacidade com o interesse público em viabilizar investigações criminais e a eficiência do processo penal impõe a exigência de que o afastamento da privacidade seja contextuai, específico e baseado em justas razões como o são os indícios de envolvimento de alguém em crime. Trata-se de mecanismo básico de controle contra arbitrariedades ao qual decisões judiciais de quebra de sigilo devem atender.

Indicam, nesse contexto, julgados desta Suprema Corte que, ante a excepcionalidade das quebras de sigilo em geral, vedam ordens de quebra de sigilo que assumam perfil de fishing expeditions: táticas investigativas de pescaria sobre quem e o que se vai investigar, por serem genéricas e lhes faltar causa provável (indícios de envolvimento em atividade criminosa) contra os afetados. Ao contrário do que supôs o Eg. STJ, não se admite o

menosprezo à privacidade de inocentes, como se fosse um dano colateral aceitável. Por isso mesmo, essa Eg. Corte já invalidou uma série de comandos de natureza indiscriminada.

Aludem à necessidade de as ordens de quebra de sigilo de dados seguirem os mesmos requisitos de restrição da privacidade, ou seja, presença de indícios de autoria e materialidade delitiva. Assim, varreduras generalizadas em históricos de pesquisa de usuários e disponibilização de listas temáticas daqueles que pesquisaram sobre certa informação representam uma intrusão inconstitucional no direito à privacidade de quem nada tem a ver com o crime investigado.

Mencionam quatro razões para demonstrar a ausência de fundamentação da decisão de quebra de sigilo de dados: (i) insuficiência, para deferimento de ordem de tamanha amplitude, da mera indicação de indícios de materialidade, (ii) inexistência de elementos concretos para justificar a adoção da medida, pois desacompanhada de elementos concretos e fundamentos inidôneos, (iii) carência de justificativa do período de 96h (noventa e seis horas) de coleta dos dados e, por fim, (iv) ausência de previsão legal de medida que autorize o fornecimento coletivo e genérico de pessoas insuspeitas para análise exploratória em um processo penal, o v. acórdão invocou o referido dispositivo do Marco Civil da Internet de forma extensiva e descontextualizada. Com efeito, o dispositivo cuida tão somente do fornecimento de registros de acesso a aplicações por parte de usuários envolvidos em ilícitos praticados na internet, justamente para que se possa identificar o responsável por determinado conteúdo específico que se aponta como ilícito. Confirmando essa constatação, o Decreto de regulamentação do Marco Civil veda textualmente que sejam feitas determinações de quebra de sigilo genéricas, exigindo a indicação dos alvos afetados (art. 11, § 3°).

Finalmente, escoram a pretensão recursal na violação do princípio da proporcionalidade por ser a medida inadequada, desnecessária e desproporcional em sentido estrito.

Asseveram a inexistência, no caso, de mecanismo de controle, pois tratamentos de dados por autoridades estatais no âmbito de investigações criminais não estão sujeitas à Lei Geral de Proteção de Dados (art. 4°, III) nem há cadeia de custódia para provas digitais prevista na legislação penal, de modo que o risco é ainda mais alto. E isso não por qualquer desconfiança específica contra as autoridades, mas por conta do próprio fluxo massivo de dados sensíveis aqui em questão.

Requerem o conhecimento e provimento do recurso extraordinário, para conceder a segurança requerida perante o TJRJ, com a consequente a cassação do item 5 da decisão proferida pelo Juízo de Direito da 4ª Vara Criminal da Comarca da Capital/RJ mantido pelas instâncias subsequentes.

É o relatório.

Presentes os pressupostos recursais intrínsecos e extrínsecos, conheço do recurso e passo ao exame quanto à existência de repercussão geral da matéria constitucional impugnada.

Em análise no presente recurso extraordinário os limites e o alcance de decisões judiciais de quebra de sigilo de dados pessoais, nas quais determinado o fornecimento de registros de acesso à internet e de IPs (internet protocol address), circunscritos a um lapso temporal demarcado, sem, contudo, a indicação de qualquer elemento concreto apto a identificar

os usuários. Em outras palavras, a possibilidade da decretação judicial da

quebra de sigilo de dados telemáticos, no âmbito de procedimentos penais, em relação a pessoas indeterminadas.

Destaco que, em diversas oportunidades, esta Suprema Corte tem se deparado com a controvérsia sobre a proteção de dados. Nesse sentido, deferi pedido de medida liminar nos autos da ADI 6.387/DF, posteriormente referendada, por maioria, pelo Plenário desta Casa.

Além disso, pendente de análise neste Tribunal a ADI 5.527/DF e a ADPF 403/SE, nas quais se discute, ainda que indiretamente, o mesmo tema de proteção de dados tendo em vista as disposições do Marco Civil da Internet (Lei 12.965/2014).

Está, pois, na agenda desta Corte o enfrentamento dos maiores desafios contemporâneos à proteção da privacidade em conflito com os imperativos de segurança nacional e da eficiência do Estado, com a proliferação de sistemas de vigilância e mídias sociais, junto com a manipulação maciça de dados pessoais em redes computacionais por inúmeros agentes públicos e privados.

Ressalto, ainda, a existência de inúmeros julgados desta Casa nos quais se delimitaram, em casos envolvendo quebra de sigilos de registros bancários, fiscais e telefônicos, busca e apreensão, os requisitos mínimos, à luz da Constituição Federal, para efetivação de tais ordens invasivas (HC 84.758/GO, Rel. Min. Celso de Mello, Tribunal Pleno, DJ 16.6.2006, v.g.).

Inegável, portanto, a presença de questão constitucional, pois a proteção de dados pessoais (art. 5º, XII, CF) na Era da Informação constitui desafio à privacidade, tudo isso alinhado à necessidade de compatibilização de quebras de sigilo de dados com os requisitos constitucionais mínimos.

De outro lado, o potencial de repetitividade do tema em análise restou devidamente comprovado pelas recorrentes, sendo indispensável o posicionamento deste Supremo Tribunal Federal sobre o tema, a fazer com que a decisão transcenda os interesses individuais atinentes à causa, com possibilidade de atingir usuários das mais diversas plataformas tecnológicas.

Ademais, saliento que esta Corte reputou constitucional e reconheceu a repercussão geral em tema análogo sobre o sigilo de comunicações telefônicas. Refiro-me ao ARE 1.042.075-RG/RJ, de relatoria do Ministro Dias Toffoli, no qual se discute a possibilidade da autoridade policial, diante de aparelho celular, obtenha acesso à agenda telefônica e ao registro de chamadas sem autorização judicial.

Ante o exposto, reconheço o caráter constitucional e a repercussão geral do tema trazido neste recurso extraordinário, submetendo o tema aos eminentes pares.

Brasília, 06 de maio de 2021.

Ministra Rosa Weber

Relatora